Diogo Filipe Pessoa da Cruz

A Conjetura de Erdős-Straus e Generalizações

Diogo Filipe Pessoa da Cruz

A Conjetura de Erdős-Straus e Generalizações

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Matemática e Aplicações, área de especialização Ciências da Computação, realizada sob a orientação científica do Dr. Paulo José Fernandes Almeida, Professor Auxiliar do Departamento de Matemática da Universidade de Aveiro

o júri / the jury

presidente / president

Professor Doutor Rui Filipe Alves Silva Duarte
Professor Auxiliar do Departamento de Matemática da Universidade de Aveiro

vogais / examiners committee

Professor Doutor Luís Filipe dos Santos Roçadas Ferreira
Professor Auxiliar do Departamento de Matemática da Escola de Ciências e Tecnologias da Universidade de Trás-os-Montes e Alto Douro

Professor Doutor Paulo José Fernandes Almeida
Professor Auxiliar do Departamento de Matemática da Universidade de Aveiro (orientador)

agradecimentos / acknowledgements

Em primeiro lugar, quero agradecer ao Dr. Paulo Almeida, com quem tive a honra e prazer de trabalhar durante o tempo em que escrevi esta dissertação. Agradeço todo o seu apoio, disponibilidade e dedicação.
Agradeço também à Universidade de Aveiro, em particular ao Departamento de Matemática, por me terem sidas disponibilizadas as condições necessárias ao desenvolvimento deste trabalho.
Por fim, quero agradecer à minha família, por todo o apoio, incentivo, paciência e compreensão que demonstraram ao longo da realização deste trabalho.

Palavras-chave Conjetura de Erdős-Straus, frações unitárias, equações diofantinas, frações egípcias.

Resumo Nesta dissertação serão apresentados os principais resultados relacionados com a conjetura de Erdős-Straus, entre os quais o teorema de Mordell. Associada à conjetura está uma equação diofantina, que iguala uma fração de numerador $n = 4$ e denominador m inteiro maior que 1, à soma de três frações unitárias. Será também analisado o número de soluções desta equação e vamos também verificar computacionalmente a validade da conjetura para $m \leq 10^9$. Finalmente, iremos ver generalizações da conjetura para qualquer n e para quando, para além de somas, podemos também ter subtrações de frações unitárias. Ambas as generalizações foram propostas por André Schinzel.

Keywords Erdős-Straus Conjecture, unit fractions, diophantine equations, egyptian fractions.

Abstract This dissertation will present the main results related to the Erdős-Straus conjecture, including the Mordell's theorem. Associated to the conjecture is a diophantine equation, that say that a fraction with numerator $n = 4$ and denominator m integer greater than 1 is equal to the sum of three unit fractions. It will be also analyzed the number of solutions of this equation and we also computationally verify the validity of the conjecture for $m \leq 10^9$. Finally, we will see generalizations of the conjecture for any n and when, in addition to sums, we also have subtractions of unit fractions. Both generalizations were proposed by André Schinzel.

Conteúdo

Capítulo 1

Preliminares

1.1 Introdução

Um dos assuntos mais importantes na área da teoria dos números é o estudo das equações diofantinas, que são equações que apenas admitem soluções inteiras. Neste trabalho, as equações diofantinas estudadas, têm que ver com frações egípcias. As frações egípcias são frações que podem ser representadas como somas de frações unitárias e têm desafiado a mente dos matemáticos desde há muito tempo, diz-se que há mais de três milénios. Nos dias de hoje, continuam ser objeto de interesse por parte dos matemáticos contemporâneos.

Este trabalho aborda uma das conjeturas ainda por provar relacionadas com frações egípcias, a conjetura formulada por Paul Erdős e Ernst G. Straus em 1948. Esta conjetura, conhecida como conjetura de Erdős-Straus, afirma que, para qualquer $m > 1$, a equação diofantina

$$\frac{4}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \tag{1.1}$$

tem solução em inteiros positivos (a, b, c). As referências mais antigas a esta conjetura vêm de P. Erdős [2] e M. R. Obláth [6]. Em 1999, A. Swett [11] verificou computacionalmente que a conjetura é válida para qualquer inteiro $m \leq 10^{14}$, sendo que, à data em que se escreve este trabalho, ninguém conseguiu verificar a validade da conjetura para um limite maior.

Associadas a esta conjetura estão duas generalizações, ambas formuladas por André Schinzel (cf. [8]). Na primeira generalização, Schinzel levanta a hipótese de que existe um inteiro positivo λ_n, onde n é um inteiro maior ou igual a 4, tal que a equação

$$\frac{n}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}$$

tem solução em inteiros positivos (a, b, c), para qualquer $m > \lambda_n$. Schinzel foi aluno de W. Sierpinski, que começou por conjeturar o caso $n = 5$.

Como já foi dito, Schinzel, formulou ainda outra generalização, esta envolvendo, para

além de somas, também subtrações. Foi então conjeturado que

$$\frac{n}{m} = \frac{1}{a} \pm \frac{1}{b} \pm \frac{1}{c}$$

tem solução em inteiros positivos (a, b, c), para qualquer $m > \mu_n$. Este caso está provado para $n < 36$, por B. M. Stewart e W. A. Webb [10].

Neste trabalho podem ser encontrados os principais resultados relacionados com a conjetura de Erdős-Straus e as suas generalizações, tendo também uma componente computacional, que envolveu a programação de rotinas no software *Maple 14*, que podem ser consultadas no apêndice A.

No restante do capítulo 1, podemos encontrar algumas noções de teoria dos números, que servirão de base para a prova de vários resultados nos capítulos seguintes.

No capítulo 2, serão introduzidos alguns resultados sobre a soma de frações unitárias, mais propriamente sobre a soma de duas e três frações unitárias. Alguns destes resultados serão bastante importantes ao longo do resto do trabalho.

No capítulo 3, vamos ver o que de mais importante foi alcançado em relação à conjetura de Erdős-Straus. Iremos observar um dos mais conhecidos teoremas sobre este tema, o teorema de Mordell, e outros dois teoremas que envolvem a soma de três frações unitárias com denominadores polinomias. Ainda neste capítulo são apresentadas propriedades da equação diofantina associada a esta conjetura, a equação (1.1). No fim temos algumas condições para que a conjetura seja válida.

O capítulo 4 é onde podemos encontrar o estudo computacional, que irá provar que a conjetura é válida para qualquer $m \leq 10^9$. Apesar de Swett já o ter feito para qualquer $m \leq 10^{14}$, pretendeu-se perceber mais promonorizadamente como podemos aplicar computacionalmente alguns dos resultados de capítulos anteriores de forma a verificar a validade da conjetura até um certo ponto.

No capítulo 5, iremos analisar o número de soluções da equação (1.1), sendo apresentados limites assintóticos para esse número e para a sua média, em particular quando temos denominador primo. Estes resultados, da autoria de C. Elsholtz e T. Tao [1], são bastante recentes, tendo sido publicados apenas em 2013.

O capítulos 6 vai ser dedicado à generalização para qualquer n e envolve também uma componente computacional.

No capítulo 7, falaremos da generalização para quando também podemos ter subtrações e vamos ver como se provam alguns dos casos particulares de n.

1.2 Noções Básicas de Teoria dos Números

Nesta secção são apresentadas algumas definições e resultados da Teoria dos Números que serão utéis ao longo deste trabalho. No livro de G. H. Hardy e E. M. Wright [3] poderão ser encontrados estes e outros conceitos da área da Teoria dos Números.

Definição 1.2.1 *Um número* primo *é um número natural maior que* 1 *que apenas é divisível por* 1 *ou por si próprio. Um número que não é primo é chamado* composto.

Definição 1.2.2 *Sejam a e b inteiros, com $a \neq 0$. Diz-se que a* divide *b, ou que b é* múltiplo *de a, se existe um inteiro c tal que $ac = b$. Denota-se por $a \mid b$.*

Teorema 1.2.3 *Sejam a, b, d, u e v inteiros, com $d \neq 0$. Se $d \mid a$ e $d \mid b$, então $d \mid au+bv$. Em particular, $d \mid a+b$, $d \mid a-b$ e $d \mid au$.*

Demonstração: Suponhamos que existem inteiros k e w tais que $a = dk$ e $b = dw$. Então

$$au + bv = dku + dwv = d(ku + wv).$$

Como $d \neq 0$ temos que $d \mid au + bv$. □

Teorema 1.2.4 *Sejam a, b e c inteiros, com $a \neq 0$ e $b \neq 0$. Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração: Se $a \mid b$ então existe um inteiro d_1 tal que $d_1 a = b$ e se $b \mid c$ então existe um inteiro d_2 tal que $d_2 b = c$. Substituindo b, temos $d_2 d_1 a = c$, logo existe um inteiro $d = d_1 d_2$ tal que $da = c$ e portanto $a \mid c$. □

Definição 1.2.5 *Sejam a e b inteiros em que pelo menos um deles é não nulo. Ao maior inteiro que divide a e b chama-se* máximo divisor comum *de a e b e denota-se por $mdc(a, b)$.*

Definição 1.2.6 *Se $mdc(a, b) = 1$ então dizemos que a e b são* coprimos *ou* primos entre si.

Axioma 1.2.7 (Princípio da boa ordenação) *Todo o conjunto não vazio de inteiros não negativos tem um elemento menor que todos os outros.*

Teorema 1.2.8 (Algoritmo da divisão) *Sejam a e b dois inteiros, com $b > 0$. Então existem unicamente dois inteiros q e r (quociente e resto, respetivamente) tais que*

i) $a = bq + r$.

ii) $0 \leq r < b$.

Demonstração: Vamos começar por provar a existência. Sejam a e b dois inteiros, com $b > 0$. Vamos considerar o conjunto

$$S = \{n \in \mathbb{Z}_0^+ : n = a - bx, x \in \mathbb{Z}\}.$$

Vamos provar que S não é um conjunto vazio. Vamos dividir a prova em dois casos, $a \geq 0$ e $a < 0$.

Se $a \geq 0$, então $a - b \times 0 = a \geq 0$, logo para $x = 0$ existe $n = a - bx$ não negativo e portanto S é não vazio quando $a \geq 0$.

Se $a < 0$, então $-a > 0$ e como b é um inteiro positivo então

$$-ab \geq -a,$$

ou seja,

$$a - ab \geq 0,$$

logo para $x = a$ existe $n = a - bx$ não negativo e portanto S também é não vazio quando $a < 0$.

Como S é subconjunto de $\mathbb{Z}_0^+$ não vazio, então, pelo princípio da boa ordenação, S contém um elemento menor que todos os outros. Seja r esse elemento e seja $x = q$, então r é da forma

$$r = a - bq,$$

ou seja,

$$a = bq + r.$$

Como $r \in S$, sabemos que $r \geq 0$. Falta ver que $r < b$. Vamos recorrer à prova por contradição. Suponhamos que $r \geq b$, então $r - b \geq 0$, logo

$$0 \leq r - b = (a - bq) - b = a - b(q + 1)$$

e portanto $r - b$ é um elemento de S. Mas como b é positivo,

$$r - b < r,$$

contradizendo a afirmação de r ser o menor elemento de S. Logo $r < b$. Provámos então a existência de inteiros q e r tal que $a = bq + r$, onde $0 \leq r < b$. Falta provar que q e r são únicos.

Suponhamos que existem dois pares de inteiros (q, r) e (q', r') tal que

$$bq + r = a = bq' + r' \tag{1.2}$$

com

$$0 \leq r, r' < b.$$

Pela equação (1.2) temos que

$$0 = bq + r - bq' - r' = b(q - q') - (r' - r),$$

ou seja,

$$b(q - q') = (r' - r). \tag{1.3}$$

Dado que b é um inteiro positivo, $(r' - r)$ é um múltiplo de b, mas como $0 \leq r, r' < b$, então $(r' - r) < b$, logo $(r' - r) = 0$, ou seja, $r = r'$. Da equação (1.3) e dado que b é positivo, tiramos que $(q - q') = 0$, ou seja, $q = q'$.

Desta forma fica provada a unicidade de q e r, completando a demonstração do teorema. □

Algoritmo de Euclides Sejam a e b dois inteiros positivos. Pelo algoritmo da divisão existem inteiros q_0 e r_0, tais que

$$a = q_0 b + r_0$$

com $0 \leq r_0 < b$.

Se $r_0 \neq 0$, pelo algoritmo da divisão existem inteiros q_1 e r_1, tais que

$$b = q_1 r_0 + r_1$$

com $0 \leq r_1 < r_0$.

Seguindo o mesmo raciocínio vamos obter uma sequência de inteiros não negativos $r_0, r_1, ..., r_k$, com $r_0 > r_1 > ... > r_k \geq 0$. Note-se que este processo termina ao fim de um número finito de passos e que o último resto, r_{k+1}, é nulo.

Teorema 1.2.9 *Sejam a e b dois inteiros positivos e r_k o último resto não nulo obtido pelo algoritmo de Euclides, então $r_k = mdc(a, b)$. Mais, o algoritmo de Euclides permite encontrar inteiros u e v tais que*

$$au + bv = mdc(a, b).$$

Demonstração: Seguindo o algoritmo de Euclides temos:

$$\begin{cases} a = bq_0 + r_0 \\ b = r_0 q_1 + r_1 \\ r_0 = r_1 q_2 + r_2 \\ ... \\ r_{k-2} = r_{k-1} q_k + r_k \\ r_{k-1} = r_k q_{k+1} \end{cases} \tag{1.4}$$

Seja $d = mdc(a, b)$. Vamos mostrar que $d \mid r_i$ e $d \mid r_{i+1}$ para qualquer $0 \leq i \leq k-1$ utilizando a prova por indução. Como $d \mid a$ e $d \mid b$, então $d \mid a - bq_0$, ou seja, $d \mid r_0$. Como $d \mid b$ e $d \mid r_0$, então $d \mid r_1$. Suponhamos agora que $d \mid r_i$ e $d \mid r_{i+1}$, queremos provar que $d \mid r_{i+1}$ e $d \mid r_{i+2}$. Por hipótese de indução, $d \mid r_i - r_{i+1} q_{i+2}$, mas $r_i - r_{i+1} q_{i+2} = r_{i+2}$ e portanto, $d \mid r_{i+2}$.

Provou-se que $d \mid r_i$ para qualquer $0 \leq i \leq k$. Em particular, $d \mid r_k$. Logo $d \leq r_k$, pois d e r_k são positivos.

Reciprocramente, a última equação de (1.4) diz-nos que $r_k \mid r_{k-1}$. Usando a penúltima equação sabemos que $r_k \mid r_{k-2}$. Por indução, podemos concluir que $r_k \mid r_i$ para qualquer $0 \leq i \leq k$. Com a segunda equação temos que $r_k \mid b$ e com a primeira, $r_k \mid a$. Logo $r_k \mid d$ e portanto, $r_k = d$.

Vamos agora provar a segunda parte do teorema. Seja $r_{-2} = a$ e $r_{-1} = b$. Sabemos que

$$r_i = r_{i-2} - r_{i-1}q_i$$

para qualquer $0 \leq i \leq k$. Vamos provar por indução que para qualquer $0 \leq i \leq k$, existem inteiros u_i e v_i tais que $r_i = u_i a + v_i b$. Dado que $r_0 = a - bq_0$ e $r_1 = b - (a - bq_0)q_1 = -q_1 a + (1 + q_0 q_1)b$ o resultado verifica-se para $i = 0$ e $i = 1$. Suponhamos que resultado também é verdadeiro para i e para $i - 1$, então

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i q_{i+1} \\ &= u_{i-1}a + v_{i-1}b - (u_i a + v_i b)q_{i+1} \\ &= (u_{i-1} - u_i q_{i+1})a + (v_{i-1} - v_i q_{i+1})b \\ &= u_{i+1}a + v_{i+1}b. \end{aligned}$$

Portanto existem inteiros u_i e v_i tais que $r_i = u_i a + v_i b$, para qualquer $0 \leq i \leq k$. Em particular, existem inteiros u e v tais que $au + bv = r_k = mdc(a, b)$. □

Teorema 1.2.10 *Se $mdc(n, a) = 1$ e $n \mid ab$, então $n \mid b$.*

Demonstração: Suponhamos que $mdc(n, a) = 1$, então, pelo teorema 1.2.9, existem inteiros u e v tais que $nu + av = 1$ e portanto, $nbu + abv = b$. Mas se $n \mid ab$, então $ab = nk$ para algum inteiro k. Logo $nbu + nkv = b$, ou seja, $n(bu + kv) = b$, e portanto, $n \mid b$. □

Teorema 1.2.11 *Se um primo divide um produto de inteiros, então divide pelo menos um dos fatores.*

Demonstração: Seja p um primo e n um inteiro maior que 1. Recorrendo à prova por indução vamos mostrar que se p dividir um produto de n inteiros, então divide pelo menos um dos fatores.

Se $n = 2$, sejam a_1 e a_2 dois inteiros e suponhamos que $p \mid a_1 a_2$. Se p dividir a_1 a afirmação é verdadeira. Caso contrário, $mdc(p, a_1) = 1$, já que, por definição de primo, os únicos divisores de p são o próprio p e 1. Então pelo teorema 1.2.10, $p \mid a_2$. A prova está então feita para $n = 2$.

Suponhamos que afirmação também é verdadeira para n=k. Sejam $a_1, a_2, ..., a_{k+1}$ inteiros tais que $p \mid a_1 a_2 ... a_{k+1}$. Se $p \mid a_{k+1}$ a afirmação verifica-se. Caso contrário, então pelas mesmas razões apresentadas anteriormente p tem de dividir o produto $a_1 a_2 ... a_k$ e por hipótese de indução tem de dividir um dos seus fatores. □

Teorema 1.2.12 *Se* $mdc(a,b) = d$, *então* $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração: Seja $k = mdc\left(\frac{a}{d}, \frac{b}{d}\right)$, onde $d = mdc(a,b)$. Então existem inteiros i e j tal que

$$\frac{a}{d} = ki \text{ e } \frac{b}{d} = kj.$$

Logo $a = kdi$ e $b = kdj$. Portanto $kd \mid a$ e $kd \mid b$. Mas como $d = mdc(a,b)$, então $kd \mid d$. Claramente $d \mid kd$, logo $kd = d$ e portanto, $k = 1$. □

Definição 1.2.13 *Sejam* a *e* b *inteiros não nulos. Ao menor inteiro positivo divisível por* a *e por* b *chama-se* mínimo múltiplo comum *de* a *e* b *e denota-se por* $mmc(a,b)$.

Proposição 1.2.14 *Sejam* a *e* b *inteiros não nulos,* $d = mdc(a,b)$ *e* $m = mmc(a,b)$. *Então*

$$md = |ab|.$$

Demonstração: Seja

$$m' = \frac{|ab|}{d}.$$

Como $d = mdc(a,b)$, então existem k, $w \in \mathbb{Z}$ tais que $a = dk$ e $b = dw$. Assim, temos que

$$m' = \frac{|a|}{d}|b| = \pm kb$$

e

$$m' = |a|\frac{|b|}{d} = \pm aw.$$

Portanto m' é múltiplo comum de a e b.

Seja um inteiro positivo c outro múltiplo comum de a e b. Então existem i, $j \in \mathbb{Z}$ tais que $c = ai = bj$. Pelo teorema 1.2.9, existem inteiros u e v tais que $au + bv = d$. Então

$$\begin{aligned}
\frac{c}{m'} &= \frac{cd}{|ab|} \\
&= \frac{c}{|ab|}(au + bv) \\
&= \frac{c}{|b|}\frac{au}{|a|} + \frac{c}{|a|}\frac{bv}{|b|} \\
&= \pm\frac{c}{b}u \pm \frac{c}{a}v \\
&= \pm ju \pm iv
\end{aligned}$$

Como podemos ver, $\frac{c}{m'}$ é inteiro, logo $m' \mid c$, o que siginifica que $m' \leq c$. Portanto

$$m' = mmc(a, b) = m$$

e temos então que $md = |ab|$. □

Teorema 1.2.15 *Seja $n > 1$ um inteiro. Então n é primo ou é um produto finito de primos.*

Demonstração: Suponhamos que existem inteiros maiores que 1 que não são primos, nem são um produto finito de primos. Seja N o menor desses inteiros. Dado que N não é primo, então é composto, logo existe um inteiro $1 < u < N$ que divide N. Assim, existe um inteiro v tal que $N = uv$. Claramente, $1 < v < N$. Portanto, por definição de N, temos que u e v são primos ou um produto finito de primos. Logo, também $uv = N$ é um produto finito de primos. Temos uma contradição e portanto, todos os inteiros maiores que 1 são primos ou um produto finito de primos. □

Teorema 1.2.16 *Seja $n > 1$ inteiro e suponhamos que*

$$n = p_1 p_2 ... p_r = q_1 q_2 ... q_s,$$

onde $p_1, p_2, ..., p_r, q_1, q_2, ..., q_s$ são primos. Então $r = s$ e as duas fatorizações de n são iguais, com a possível exceção da ordem dos fatores.

Demonstração: Recorrendo à prova por contradição, vamos supor que o teorema é falso. Seja N o menor inteiro para o qual o teorema é falso. Então o teorema é verdadeiro para qualquer inteiro $1 < n < N$. Suponhamos que

$$N = p_1 p_2 ... p_r = q_1 q_2 ... q_s, \tag{1.5}$$

onde $p_1, p_2, ..., p_r, q_1, q_2, ..., q_s$ são primos. Como claramente o teorema é verdadeiro para números primos, então N é composto. Portanto $r, s \geq 2$. Dado que a ordem dos fatores não importa, podemos assumir que

$$p_r \geq p_i, \ 1 \leq i \leq r - 1$$

e

$$q_s \geq p_j, \ 1 \leq j \leq s - 1.$$

Vamos começar por provar que não podemos ter $p_r > q_s$. Se $p_r > q_s$, então $p_r > p_j$, para qualquer $1 \leq j \leq s$. Portanto, $p_r \nmid q_j$, para qualquer $1 \leq j \leq s$. Mas

$$p_r \mid q_1 q_2 ... q_s,$$

contradizendo o teorema 1.2.11. Logo $p_r \leq q_s$. De forma análoga, iríamos obter uma contradição se $p_r < q_s$. Portanto, $p_r = q_s$.

De (1.5), temos

$$\frac{N}{p_r} = p_1 p_2 ... p_{r-1} = q_1 q_2 ... q_{s-1}$$

e

$$1 < \frac{N}{p_r} < N,$$

pois $r, s \geq 2$. Então o teorema é válido para $\frac{N}{p_r}$, isto é, $r - 1 = s - 1$ e as fatorizações de $p_1 p_2 ... p_{r-1}$ e $q_1 q_2 ... q_{s-1}$ são iguais, com a possível exceção da ordem dos fatores. Portanto, $r = s$ e, como $p_r = q_s$, as fatorizações de N em primos são iguais, com a possível exceção da ordem dos fatores. Logo o teorema é válido para N, contradizendo a definição de N.

Portanto, o teorema é válido para qualquer inteiro $n > 1$. □

Definição 1.2.17 *Sejam a, b e n inteiros, com $n > 1$. Diz-se que a é* congruente *com b módulo n, e denota-se $a \equiv b \bmod n$, se $n \mid b - a$. Por abuso de notação, ao longo do texto iremos escrever $a = b \bmod n$.*

Teorema 1.2.18 *Se $mdc(a, n) = d$ e $ab = ac \bmod n$, então*

$$b = c \bmod \frac{n}{d}.$$

Demonstração: Suponhamos que $mdc(a, n) = d$ e $ab = ac \bmod n$, então

$$ab = ac + kn \tag{1.6}$$

para k inteiro. Sejam

$$a_1 = \frac{a}{d} \text{ e } n_1 = \frac{n}{d}$$

Claramente a_1 e n_1 são inteiros e $mdc(a_1, n_1) = 1$. Dividindo ambos os membros da equação (1.6) por d, temos $a_1(b - c) = kn_1$, logo $a_1 \mid kn_1$. Já vimos que $mdc(a_1, n_1) = 1$, logo pelo teorema (1.2.10), $a_1 \mid k$. Portanto, $k = a_1 k_1$, para k_1 inteiro. Assim, $b - c = k_1 n_1$, logo $n_1 \mid b - c$. Portanto, $b = c \bmod \frac{n}{d}$. □

Definição 1.2.19 *Seja p um primo e n um inteiro não negativo, então definimos* valuação p-ádica de n *como*

$$\upsilon_p(n) = \max\{v : p^v \mid n\}$$

Definição 1.2.20 *Seja x um número real, definimos* chão de x *como o maior inteiro menor ou igual que x e denotamos por $\lfloor x \rfloor$, isto é*

$$\lfloor x \rfloor = \max\{m \in \mathbb{Z} : m \leq x\}$$

Definimos teto de x *como menor inteiro maior ou igual que x e denotamos por $\lceil x \rceil$, isto é*

$$\lceil x \rceil = \min\{n \in \mathbb{Z} : n \geq x\}$$

Capítulo 2

Somas de Frações Unitárias

Neste capítulo serão introduzidos alguns resultados relacionados com a soma de frações unitárias. Primeiro serão apresentados resultados para a soma de duas frações unitárias e depois para a soma de três frações unitárias. Estes resultados terão grande importância ao longo do trabalho. Mas antes, vejamos a definição de fração unitária:

Definição 2.0.21 *A uma fração na forma* $\frac{1}{k}$*, com* k *inteiro positivo, chama-se* fração unitária.

2.1 Soma de Duas Frações Unitárias

O seguinte teorema garante condições necessárias e suficientes que permitem descobrir se uma fração pode ser escrita como a soma de duas frações unitárias.

Teorema 2.1.1 *Sejam* n *e* $m \in \mathbb{Z}^+$ *coprimos. Então*

$$\frac{n}{m} = \frac{1}{x} + \frac{1}{y} \tag{2.1}$$

para x*,* $y \in \mathbb{Z}^+$ *se e só se existem inteiros* d_1 *e* d_2 *tal que*

i) d_1*,* $d_2 \mid m$

ii) $n \mid d_1 + d_2$

Demonstração: Suponhamos que existem inteiros d_1 e d_2 divisores de m com $n \mid d_1 + d_2$. Então $m = id_1 = jd_2$ e $d_1 + d_2 = kn$, para i, j, $k \in \mathbb{Z}^+$. Assim,

$$\begin{aligned} \frac{n}{m} &= \frac{kn}{km} \\ &= \frac{d_1}{mk} + \frac{d_2}{mk} \\ &= \frac{d_1}{id_1k} + \frac{d_2}{jd_2k} \\ &= \frac{1}{ik} + \frac{1}{jk} \end{aligned}$$

Temos a igualdade pretendida com

$$x = ik = k\left(\frac{m}{d_1}\right)$$

e

$$y = jk = k\left(\frac{m}{d_2}\right)$$

Suponhamos agora que $\frac{n}{m} = \frac{1}{x} + \frac{1}{y}$, para x e $y \in \mathbb{Z}^+$. Seja $d = mdc(x, y)$, com $x = dx_0$ e $y = dy_0$, para inteiros x_0 e y_0. Então

$$\frac{nd}{m} = \frac{d}{dx_0} + \frac{d}{dy_0} = \frac{1}{x_0} + \frac{1}{y_0} = \frac{x_0 + y_0}{x_0 y_0} \tag{2.2}$$

Vamos agora ver que $mdc(x_0 + y_0, x_0y_0) = 1$. Suponhamos que existe um primo q que divide $x_0 + y_0$ e x_0y_0. Então q também divide $x_0(x_0 + y_0) - x_0y_0 = x_0^2$ e portanto, pelo teorema 1.2.11, $q \mid x_0$. De forma análoga $q \mid y_0$. Mas pelo teorema 1.2.12, $mdc(x_0, y_0) = 1$, logo temos uma contradição. Deste modo, não há primos que dividam $x_0 + y_0$ e x_0y_0, portanto, $mdc(x_0 + y_0, x_0y_0) = 1$.

Da equação (2.2) temos que

$$ndx_0y_0 = m(x_0 + y_0), \tag{2.3}$$

logo, $x_0y_0 \mid m(x_0 + y_0)$. Já vimos que $mdc(x_0 + y_0, x_0y_0) = 1$, então pelo teorema 1.2.10, $x_0y_0 \mid m$. Claramente $x_0 \mid x_0y_0$ e $y_0 \mid x_0y_0$, então pelo teorema 1.2.4, $x_0 \mid m$ e $y_0 \mid m$.

Vamos agora mostrar que $n \mid x_0 + y_0$. Tendo em conta a equação (2.3) temos que $n \mid m(x_0 + y_0)$. Mas como $mdc(n, m) = 1$, pelo teorema 1.2.10, $n \mid x_0 + y_0$. Tomando $d_1 = x_0$ e $d_2 = y_0$, temos o resultado pretendido.

O teorema está então provado. □

A seguir vamos verificar que podemos sempre escrever uma fração unitária como uma soma de duas:

Observação 2.1.2 *Claramente*

$$\frac{1}{x} = \frac{1}{2x} + \frac{1}{2x},$$

para qualquer inteiro positivo x.

De notar que também é possível obter uma soma de duas frações unitárias com denominadores diferentes, basta ver que

$$\frac{1}{x} = \frac{1}{x+1} + \frac{1}{x(x+1)},$$

para qualquer inteiro positivo x.

2.2 Soma de Três Frações Unitárias

Nesta secção serão apresentados resultados sobre a soma de três frações unitárias, mais propriamente sobre a equação

$$\frac{n}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}, \tag{2.4}$$

onde $n \geq 4$, m e $a \leq b \leq c$ são inteiros positivos.

Vejamos agora a seguinte observação:

Observação 2.2.1 *É fácil verificar que na equação (2.4) temos*

$$\frac{n}{m} > \frac{1}{a},$$

pois b e c são positivos. Logo $a > \frac{m}{n}$. Também é possível ver que

$$\frac{n}{m} \leq \frac{3}{a},$$

pois $a \leq b \leq c$. Logo $a \leq \frac{3m}{n}$. Portanto temos que

$$\frac{m}{n} < a \leq \frac{3m}{n}.$$

Esta observação e o teorema 2.1.1 permitem afirmar o seguinte:

Corolário 2.2.2 *Sejam n e m inteiros positivos, então é possível decidir num número finito de passos se $\frac{n}{m}$ pode ser escrito na forma*

$$\frac{n}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}$$

para a, b e c inteiros positivos e $a \leq b \leq c$

Demonstração: Como vimos na observação 2.2.1 há um número finito de valores de a possíveis. Para cada valor de a basta então testar se

$$\frac{n}{m} - \frac{1}{a} = \frac{na - m}{ma}$$

pode ser escrita como soma de duas frações unitárias. Para tal, de acordo com o teorema 2.1.1 basta saber se existem divisores de ma tais que $na - m$ divide a sua soma. Mas como o número de divisores é finito[1], o teste é completo e finito. □

A seguir é apresentado um importante lema:

Lema 2.2.3 *Se a equação (2.4) tem solução para m, então também tem solução para qualquer múltiplo de m.*

Demonstração: É facil verificar este lema, uma vez que se tivermos

$$\frac{n}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c},$$

então

$$\frac{n}{km} = \frac{1}{ka} + \frac{1}{kb} + \frac{1}{kc},$$

para qualquer inteiro positivo k. □

Tendo em conta o lema anterior, a partir de agora iremos apenas ver os casos em que m é primo e passaremos a lidar com a equação

$$\frac{n}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \tag{2.5}$$

com p primo. Mas atenção, pois se esta equação não tiver solução para um certo primo p, poderá também não ter para um composto múltiplo desse p e esses casos terão de tratados à parte.

O limite superior de a visto na observação 2.2.1 pode ser melhorado como podemos ver no seguinte teorema apresentado por William A. Webb em [12]:

Teorema 2.2.4 *Seja $n \geq 4$, p um primo ímpar tal que $mdc(n, p) = 1$ e sejam $a \leq b \leq c$ inteiros positivos que verificam a equação (2.5). Então*

$$a \leq \frac{2p + 2}{n}$$

[1] O número de divisores de um inteiro positivo n é $d(n) = \prod_{i=1}^{w(n)}(1 + \alpha_i)$, onde $w(n)$ é o número de fatores primos p_i de n e α_i é o expoente de p_i na fatorização de n.

Mais, se $a > \frac{2p}{n}$, *então ou* $n \mid 2p+1$ *e* $a = \dfrac{2p+1}{n}$, *ou* $n \mid p+1$ *e* $a = \dfrac{2p+2}{n}$

Demonstração: Pelo teorema 2.1.1

$$\frac{n}{p} - \frac{1}{a} = \frac{na-p}{pa} = \frac{1}{b} + \frac{1}{c} \tag{2.6}$$

se e só se existem inteiros d_1 e d_2 tal que $d_1, d_2 \mid pa$ e $na - p \mid d_1 + d_2$. A segunda condição garante a existência de um inteiro s tal que $d_1 + d_2 = s(na-p)$. Fazendo $k = na - p$ e $m = pa$, pela prova do referido teorema ficamos a saber que

$$b = s\left(\frac{m}{d_1}\right) \text{ e } c = s\left(\frac{m}{d_2}\right)$$

e portanto temos

$$\frac{k}{m} = \frac{1}{s\left(\frac{m}{d_1}\right)} + \frac{1}{s\left(\frac{m}{d_2}\right)}. \tag{2.7}$$

Como $a \leq b \leq c$, então

$$a \leq s\left(\frac{m}{d_1}\right) \leq s\left(\frac{m}{d_2}\right).$$

Vamos assumir agora que $a > \dfrac{2p}{n}$. Então $na - p > p$. Da observação 2.2.1, sabemos que

$$a \leq \frac{3p}{n}$$

e como $n \geq 4$,

$$a \leq \frac{3p}{4},$$

logo $p \nmid a$. Assim, $mdc(p, na) = 1$ e portanto, $mdc(p, na-p) = 1$.

Sejam u e v dois inteiros positivos divisores de a, com $u \leq v$. Recorrendo à prova por contradição vamos mostrar que $na - p \nmid u + v$.

Vamos assumir que $na - p \mid u + v$, então $na - p \leq u + v$. Mas

$$u + v \leq 2a \leq \frac{3}{2}p < \frac{3}{2}(na - p),$$

logo

$$na - p = u + v. \tag{2.8}$$

Temos ainda que se $v < a$, então

$$u + v \leq a < p < na - p,$$

contradizendo a equação (2.8), logo $v = a$.

Portanto, substituindo v por a na equação (2.8), temos $u = (n-1)a - p$, logo $u \mid (n-1)a - p$ e visto que $u \mid a$, então $u \mid p$. Como $mdc(p, a) = 1$, então $u = 1$. Assim,

$$a = \frac{p+1}{n-1} \leq \frac{2p}{n}$$

e temos uma contradição. Logo $na - p \nmid u + v$.

Uma vez que $d_1, d_2 \mid pa$ e $na - p \mid d_1 + d_2$, como vimos acima, d_1 e d_2 não podem dividir só a. Também não podemos ter $d_1 = pd_3$ e $d_2 = pd_4$ com $d_3, d_4 \mid a$, pois assim teríamos $na - p \mid p(d_3 + d_4)$ e como $mdc(p, na - p) = 1$, isso implicaria que $na - p \mid d_3 + d_4$, contradizendo mais uma vez o que vimos acima. Portanto, visto que $d_1 \geq d_2$ já que $b \leq c$, temos que $d_1 = pd$, com $d \mid a$ e $d_2 \mid a$.

Sabemos então que

$$pd + d_2 = s(na - p) > sp$$

e

$$d_2 \leq a < p,$$

logo $pd + p > sp$, isto é, $d + 1 > s$ e como d é inteiro,

$$d \geq s.$$

Portanto

$$\frac{sm}{d_1} = \frac{spa}{pd} = \frac{sa}{d} \leq a,$$

mas como já vimos, $a \leq \frac{sm}{d_1}$, então

$$a = \frac{sm}{d_1} = b.$$

Substituindo b por a na equação (2.6), temos

$$\frac{n}{p} - \frac{2}{a} = \frac{na - 2p}{pa} = \frac{1}{c} \tag{2.9}$$

e portanto, $na - 2p \mid pa$.

É fácil ver que $mdc(p, na-2p) = 1$, logo $na-2p \mid a$ e portanto, $na-2p \mid na$. Claramente, $na - 2p \mid na - 2p$, então, pelo teorema 1.2.3, $na - 2p \mid 2p$, o que implica que $na - 2p = 1$ ou 2. Se $na - 2p = 1$, então $n \mid 2p + 1$ e

$$a = \frac{2p+1}{n}.$$

Se $na - 2p = 2$, então

$$n\frac{a}{2} = p + 1$$

e a equação (2.9) verifica-se se e só se a é par. Deste modo, $\frac{a}{2}$ é inteiro e portanto, $n \mid p+1$ e

$$a = \frac{2p+2}{n}.$$

O teorema está assim provado. □

Num trabalho de Maria Monks e Ameya Velingker, [4], é possível encontrar o seguinte teorema, no qual podemos ver algumas propriedades relacionadas com a soma de três frações unitárias.

Teorema 2.2.5 *Sejam $n \geq 4$ um inteiro, $p > n$ um primo e (a, b, c) uma solução de inteiros positivos para a equação (2.5) com $a \leq b \leq c$.*

Então as seguintes propriedades verificam-se:

1. *Seja $q \neq p$ um primo. Então pelo menos dois dos valores $v_q(a)$, $v_q(b)$ e $v_q(c)$ são iguais a $\max\{v_q(a), v_q(b), v_q(c)\}$.*

2. *Seja q um inteiro positivo tal que o $mdc(q, p) = 1$. Se q divide um dos valores a, b ou c então q divide o produto dos restantes dois.*

3. *$a < p$, $p \nmid a$ e $p \mid c$.*

Demonstração:

1. Seja $t = \max\{v_q(a), v_q(b), v_q(c)\}$. Dado a afirmação ser simétrica em relação a a, b e c, assume-se sem perda de generalidade que $t = v_q(a)$. Por definição de máximo temos $v_q(c) \leq t$, e dado que no caso de $v_q(c) = t$ o resultado está provado, basta ter em atenção o caso em que $v_q(c) < t$.

   Sejam $s = v_q(b)$ e $r = v_q(c)$. Então temos $a = q^t a'$, $b = q^s b'$ e $c = q^r c'$, para algum a', b', $c' \in \mathbb{Z}^+$. Temos ainda que a', b' e c' são coprimos com q. Atribuindo estes valores na equação (2.5) temos:

   $$\frac{n}{p} = \frac{1}{q^t a'} + \frac{1}{q^s b'} + \frac{1}{q^r c'}$$

   ou seja,

   $$nq^r c' = p\left(\frac{q^r c'}{q^t a'} + \frac{q^r c'}{q^s b'} + 1\right),$$

   portanto,

   $$nq^r c' - p = pq^r c'\left(\frac{1}{q^t a'} + \frac{1}{q^s b'}\right),$$

   assim,

   $$nq^r c' - p = pq^r c'\left(\frac{q^s b' + q^t a'}{q^t a' q^s b'}\right),$$

logo,

$$(nq^r c' - p)q^t a'b' = pq^r c'(b' + q^{t-s}a').$$

Daqui sai que

$$v_q(pq^r c'(b' + q^{t-s}a')) = v_q((nq^r c' - p)q^t a'b') \geq t.$$

Por hipótese, $t > r$ e, por transitividade,

$$v_q(pq^r c'(b' + q^{t-s}a')) > r.$$

Portanto, $q \mid pc'(b' + q^{t-s}a')$. Por definição de primo, $mdc(q, p) = 1$, e como vimos acima que $mdc(q, c') = 1$, então $q \mid b' + q^{t-s}a'$.

Assumindo que $s < t$, temos que $q \mid q^{t-s}a'$ e portanto $q \mid b'$, o que contradiz o facto do $mdc(q, b') = 1$. Logo, uma vez que, por definição de máximo, $s \leq t$, então $s = t$ garantindo o resultado pretendido.

2. Seja q um inteiro positivo coprimo com p. Suponhamos que q divide c. Então $c = qc'$ para algum $c' \in \mathbb{Z}^+$. Substituindo na equação (2.5) temos:

$$\frac{n}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{qc'},$$

ou seja,

$$n = \frac{pa + pb}{ab} + \frac{p}{qc'},$$

portanto,

$$(nab - pa - pb) = \frac{pab}{qc'}$$

logo,

$$(nab - pa - pb)qc' = pab.$$

Portanto, $q \mid pab$ e, como q e p são coprimos, então $q \mid ab$. Analogamente se prova que qualquer divisor de b coprimo com p divide ac e qualquer divisor de a coprimo com p divide bc.

3. Claramente, se $a < p$, então $p \nmid a$. Vamos começar então por povar que $a < p$.

   Como $n \geq 4$ e atendendo à observação 2.2.1,

$$a \leq \frac{3p}{4} < p,$$

Falta então provar que $p \mid c$. Note-se que da equação (2.5) se tira que

$$\frac{n}{p} = \frac{bc + ac + ab}{abc},$$

logo,

$$nabc = p(bc + ac + ab),$$

o que implica que $p \mid nabc$. Como $p > n$ é primo, $mdc(p, n) = 1$, logo $p \mid abc$. A primalidade de p implica também que $p \mid a$ ou $p \mid b$ ou $p \mid c$. Já sabemos que $p \nmid a$, portanto, $p \mid b$ ou $p \mid c$.

Assuma-se que $p \nmid c$, então $p \mid b$ e portanto existe um inteiro positivo k tal que $b = pk$. Por hipótese, c é um divisor de c coprimo com p, logo, por (2.), temos que $c \mid ab$, ou seja, $c \mid apk$. Como c e p são coprimos , $c \mid ak$, logo $c \leq ak$. Também já vimos que $a < p$, então,

$$c \leq ak < pk = b.$$

Mas $b \leq c$ e portanto temos uma contradição. Logo $p \mid c$.

□

Capítulo 3

Conjetura de Erdős-Straus

Neste capítulo irão ser apresentados diversos resultados relacionados com a conjetura de Erdős-Straus e com a equação a que está associada. Como foi já foi referido na introdução, a conjetura afirma que para qualquer inteiro positivo $m > 1$, temos

$$\frac{4}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}, \tag{3.1}$$

para a, b e c inteiros positivos.

Um dos resultados mais relevantes é o teorema de Mordell, sendo também apresentados resultados sobre a soma de três frações unitárias com denominadores polinomiais. Serão depois referidas propriedades da equação (3.1), quando m é primo e maior que 4. No fim serão apresentadas condições para que a conjetura de Erdős-Straus seja válida.

3.1 Teorema de Mordell

Em 1968, Mordell [5] conseguiu demonstrar que a conjetura de Erdős-Straus era sempre verificada para quaquer inteiro $m > 1$, exceto, possivelmente, quando o m é primo e congruente com $1^2, 11^2, 13^2, 17^2, 19^2$ ou 23^2 mod 840.

A seguir são apresentados os vários lemas que levam ao resultado de Mordell.

Lema 3.1.1 *Sejam m, a, b, c e d inteiros positivos, com $m > 1$. Se*

$$ma + b + c = 4abcd, \tag{3.2}$$

então

$$\frac{1}{bcd} + \frac{1}{acdm} + \frac{1}{abdm} = \frac{4}{m}.$$

Demonstração: Pegando na equação (3.2) temos

$$\frac{ma}{abcd} + \frac{b}{abcd} + \frac{c}{abcd} = 4,$$

ou seja,

$$\frac{m}{bcd} + \frac{1}{acd} + \frac{1}{abd} = 4,$$

e dividindo todos os termos por m, temos

$$\frac{1}{bcd} + \frac{1}{acdm} + \frac{1}{abdm} = \frac{4}{m}.$$

□

Lema 3.1.2 *A equação (3.1) tem solução para qualquer* $m \neq 1 \bmod 4$.

Demonstração: Podemos verificar que se $m = 4a$ então $\frac{4}{m}=\frac{1}{a}$, logo $\frac{4}{m}$ pode ser expresso por uma única fração unitária e tendo em conta a observação 2.1.2, facilmente percebemos que também por três frações unitárias. Logo, a equação (3.1) tem solução para qualquer $m = 0 \bmod 4$.

Na equação (3.2) podemos atribuir os valores $a = 2$ e $b = c = 1$ e ficamos com $2m + 1 + 1 = 8d$, ou seja, $m = 4d - 1$. Tendo em conta o lema 3.1.1, verificamos que $\frac{4}{m}$ pode ser expresso como soma de três frações unitárias. Assim, a equação (3.1) tem solução para qualquer $m = 3 \bmod 4$.

Se agora atribuirmos os valores $a = b = c = 1$, temos $m = 4d - 2$, e verificamos assim que a equação (3.1) tem solução para qualquer $m = 2 \bmod 4$.

Portanto, a equação (3.1) tem solução para qualquer $m \neq 1 \bmod 4$. □

Vamos agora ver que, atendendo à prova deste lema, podemos descobrir como se escreve um inteiro congruente com 3 mod 4 como soma de três frações unitárias:

Exemplo 3.1.3 *Seja* $m = 383$*, então* $m = 3 \bmod 4$*. Pela prova do lema anterior e pelo lema 3.1.1, se na equação (3.2),* $a = 2$*,* $b = c = 1$ *e* d *é tal que* $m = 4d-1$*, ou seja* $d = 96$*, temos que*

$$\frac{4}{383} = \frac{1}{1 \times 1 \times 96} + \frac{1}{2 \times 1 \times 96 \times 383} + \frac{1}{2 \times 1 \times 96 \times 383},$$

ou seja,

$$\frac{4}{383} = \frac{1}{96} + \frac{1}{73536} + \frac{1}{73536}.$$

Vejamos os restantes lemas, que dadas as suas provas, podem levar a exemplos como o anterior:

Lema 3.1.4 *A equação (3.1) tem solução para qualquer* $m \neq 1 \bmod 8$.

Demonstração: Tendo em conta o lema 3.1.2 temos que a equação (3.1) tem solução para qualquer $m \neq 1$ ou 5 mod 8. Falta então provar que a equação (3.1) tem solução para qualquer $m = 5 \bmod 8$.

Para tal, atribuimos na equação (3.2) os valores $a = b = 1$ e $c = 2$. Assim ficamos com $m = 8d - 3$, e portanto, pelo lema 3.1.1, a equação (3.1) tem solução para qualquer $m = 5 \bmod 8$.

Portanto, a equação (3.1) tem solução para qualquer $m \neq 1 \bmod 8$. □

Lema 3.1.5 *A equação (3.1) tem solução para qualquer* $m \neq 1 \bmod 3$.

Demonstração: Pegando na equação (3.2) podemos obter a seguinte equação equivalente:

$$ma + b = (4abd - 1)c \tag{3.3}$$

Atribuindo a esta equação os valores $a = b = d = 1$, temos $m + 1 = 3c$, e portanto, $m = 3c - 1$. Logo, tendo em conta o lema 3.1.1, a equação (3.1) tem solução para $m = 2 \bmod 3$.

Como podemos verificar que $\frac{4}{3} = \frac{1}{1} + \frac{1}{4} + \frac{1}{12}$, então, pelo lema 2.2.3, a equação (3.1) tem solução para qualquer múltiplo de m, ou seja, para qualquer $m = 0 \bmod 3$.

Portanto, a equação (3.1) tem solução para qualquer $m \neq 1 \bmod 3$. □

Lema 3.1.6 *A equação (3.1) tem solução para qualquer* $m \neq 1, 2$ *ou* $4 \bmod 7$.

Demonstração: Se na equação (3.3) atribuirmos os valores:

- $a = 1$, $b = 2$ e $d = 1$, então $m + 2 = 7c$, logo $m = -2 \bmod 7$ e portanto, pelo lema 3.1.1, a equação (3.1) tem solução para qualquer $m = 5 \bmod 7$.
- $a = 2$, $b = 1$ e $d = 1$, então $2m + 1 = 7c$, logo $2m = 6 \bmod 7$, ou seja, $m = 3 \bmod 7$ e portanto, pelo lema 3.1.1, a equação (3.1) tem solução para qualquer $m = 3 \bmod 7$.
- $a = 1$, $b = 1$ e $d = 2$, então $m + 1 = 7c$, logo $m = -1 \bmod 7$ e portanto, pelo lema 3.1.1, a equação (3.1) tem solução para qualquer $m = 6 \bmod 7$.

Como $\frac{4}{7} = \frac{1}{2} + \frac{1}{15} + \frac{1}{210}$, então, pelo lema 2.2.3, a equação (3.1) tem solução para qualquer $m = 0 \bmod 7$.

Portanto, a equação (3.1) tem solução para qualquer $m \neq 1, 2$ ou $4 \bmod 7$. □

Vejamos mais um exemplo:

Exemplo 3.1.7 *Seja* $m = 83$*, então* $m = 6 \bmod 7$*. Pela prova do lema anterior e pelo lema 3.1.1, se na equação (3.2),* $a = b = 1$*,* $d = 2$ *e* c *é tal que* $m + 1 = 7c$*, ou seja* $c = 12$*, temos que*

$$\frac{4}{83} = \frac{1}{1 \times 12 \times 2} + \frac{1}{1 \times 12 \times 2 \times 83} + \frac{1}{1 \times 1 \times 2 \times 83},$$

ou seja,

$$\frac{4}{383} = \frac{1}{24} + \frac{1}{1992} + \frac{1}{166}.$$

Antes do teorema de Mordell temos ainda o seguinte lema:

Lema 3.1.8 *A equação (3.1) tem solução para qualquer* $m \neq 1$ *ou* $4 \bmod 5$.

Demonstração: Como o lema 3.1.5 garante que a equação (3.1) tem solução para qualquer $m \neq 1 \bmod 3$, então também tem solução para qualquer $m \neq 1, 4, 7, 10$ ou $13 \bmod 15$. Se na equação (3.3) atribuirmos os valores:

- $a = 1$, $b = 2$ e $d = 2$, então $m + 2 = 15c$, logo $m = 13 \bmod 15$ e portanto, pelo lema 3.1.1, a equação (3.1) tem solução para qualquer $m = 13 \bmod 15$.
- $a = 2$, $b = 1$ e $d = 2$, então $2m+1 = 15c$, logo $2m = 14 \bmod 15$, ou seja, $m = 7 \bmod 15$ e portanto, pelo lema 3.1.1, a equação (3.1) tem solução para qualquer $m = 7 \bmod 15$.

Podemos ver que a equação (3.1) tem solução para qualquer $m \neq 1, 4$ ou $10 \bmod 15$, e portanto, para qualquer $m \neq 0, 1$ ou $4 \bmod 5$.

Mas temos ainda que $\frac{4}{5} = \frac{1}{2} + \frac{1}{5} + \frac{1}{10}$, então, pelo lema 2.2.3, a equação (3.1) tem solução para qualquer $m = 0 \bmod 5$.

Portanto, a equação (3.1) tem solução para qualquer $m \neq 1$ ou $4 \bmod 5$. □

Podemos agora chegar ao teorema de Mordell:

Teorema 3.1.9 *A equação (3.1) tem solução em inteiros positivos para qualquer inteiro* $m > 1$ *exceto, possivelmente, para* m *congruente com* $1^2, 11^2, 13^2, 17^2, 19^2$ *ou* $23^2 \bmod 840$.

Demonstração: Se tivermos em conta os lemas 3.1.4 e 3.1.5, verificamos que a equação (3.1) tem solução para qualquer $m \neq 1 \bmod 24$, e portanto, também para qualquer

$$m \neq 1, 25, 49, 73 \text{ ou } 97 \bmod 120.$$

Mas podemos ver que o lema 3.1.8 também garante que a equação (3.1) tem solução para qualquer $m \neq 1$ ou $49 \bmod 120$ e portanto, para qualquer

$$m \neq 1, 49, 121, 169, 241, 289, 361, 409, 481, 529, 601, 649, 721 \text{ ou } 769 \bmod 840.$$

Se ainda juntarmos o lema 3.1.6 podemos observar que a equação (3.1) tem solução para qualquer $m \neq 1, 121, 169, 289, 361$ ou 529 mod 840, ou seja, para qualquer

$$m \neq 1^2, 11^2, 13^2, 17^2, 19^2 \; ou \; 23^2 \text{ mod } 840.$$

□

3.2 Somas de Três Frações Unitárias com Denominadores Polinomiais

Nesta secção serão apresentados dois teoremas relacionados com a soma de três frações unitárias com denominadores polinomias. O primeiro teorema, utilizado por Swett [11] no seu estudo, permite obter uma grande quantidade de inteiros positivos m que satisfazem a equação

$$\frac{4}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}, \tag{3.4}$$

para inteiros positivos a, b e c. Ou seja, se houver um limite de pesquisa por inteiros para os quais a conjetura de Erdős-Straus é válida, com o teorema, a quantidade de inteiros a verificar para o mesmo limite será bastante menor. Isto será aplicado computacionalmente no capítulo seguinte.

O segundo teorema pode explicar porque é que no teorema de Mordell, as exceções são resíduos quadráticos.

Vejamos então o primeiro teorema:

Teorema 3.2.1 *Sejam m e k inteiros positivos, $z = 4k - 1$ e u e v dois inteiros coprimos divisores de k. Se*

$$um + v = 0 \text{ mod } z, \tag{3.5}$$

então para qualquer inteiro positivo n, existem três polinómios positivos $f(x)$, $g(x)$ e $h(x)$ tais que

$$\frac{4}{nzx + m} = \frac{1}{f(x)} + \frac{1}{g(x)} + \frac{1}{h(x)} \tag{3.6}$$

e $f(0)$, $g(0)$ e $h(0)$ são inteiros positivos.

Demonstração: Suponhamos que u e v são coprimos e divisores de k, então existe um inteiro d tal que $duv = k$. Suponhamos ainda que $um + v = 0$ mod z, então existe r inteiro positivo tal que $um + v = zr$. Sejam $f(x) = k(znx + m)$, $g(x) = dv(unx + r)$ e

$h(x) = du(znx + m)(unx + r)$ três polinómios positivos. Então temos que:

$$\begin{aligned}
\frac{1}{g(x)} + \frac{1}{h(x)} &= \frac{1}{dv(unx + r)} + \frac{1}{du(znx + m)(unx + r)} \\
&= \frac{u(znx + m) + v}{duv(znx + m)(unx + r)} \\
&= \frac{uznx + um + v}{duv(znx + m)(unx + r)} \\
&= \frac{uznx + zr}{k(znx + m)(unx + r)} \\
&= \frac{z(unx + r)}{k(znx + m)(unx + r)} \\
&= \frac{z}{k(znx + m)}
\end{aligned}$$

mas,

$$\begin{aligned}
\frac{4}{nzx + m} - \frac{1}{f(x)} &= \frac{4}{nzx + m} - \frac{1}{k(znx + m)} \\
&= \frac{4k - 1}{k(znx + m)} \\
&= \frac{z}{k(znx + m)} \\
&= \frac{1}{g(x)} + \frac{1}{h(x)}
\end{aligned}$$

logo a equação (3.6) é verificada.

De notar ainda que $f(0) = km$, $g(0) = dvr$ e $h(0) = dumr$ são todos inteiros positivos. □

Se no teorema 3.2.1 atribuirmos a x o valor 0 temos o seguinte resultado:

Corolário 3.2.2 *Sejam m e k inteiros positivos e u e v dois inteiros coprimos divisores de k. Se*

$$um + v = 0 \bmod (4k - 1), \tag{3.7}$$

então a equação (3.4) tem solução para m, com

$$\frac{4}{m} = \frac{1}{km} + \frac{1}{dvr} + \frac{1}{dumr},$$

onde d é um inteiro tal que $duv = k$ e r um inteiro positivo tal que $um + v = (4k - 1)r$.

Vejamos agora o exemplo de um primo, $m = 1009 = 169 \bmod 840$, que está nas exceções do teorema de Mordell, mas para o qual o corolário anterior arranja solução:

Exemplo 3.2.3 *Sejam $m = 1009$, $u = 1$, $v = 3$ e $k = 3$. Então*

$$um + v = 0 \bmod (4k - 1) \tag{3.8}$$

Pelo corolário anterior, temos $d = 1$ e $r = 92$ e portanto

$$\frac{4}{1009} = \frac{1}{3 \times 1009} + \frac{1}{1 \times 3 \times 92} + \frac{1}{1 \times 1 \times 1009 \times 92},$$

ou seja,

$$\frac{4}{1009} = \frac{1}{3027} + \frac{1}{276} + \frac{1}{92828}.$$

Vejamos agora o que é um resíduo quadrático:

Definição 3.2.4 *Sejam a e n inteiros tais que $n > 0$ e $n \nmid a$. Se a congruência*

$$x^2 = a \bmod n$$

tiver soluções, dizemos que a é um resíduo quadrático *de n.*

O teorema seguinte foi apresentado por Schinzel em [7] e pode explicar o facto de no teorema de Mordell apenas termos resíduos quadráticos como exceções:

Teorema 3.2.5 *Sejam u e v inteiros, com u positivo e $mdc(u, v) = 1$. Se v é um resíduo quadrárico* mod u*, então não existem polinomiais F_1, F_2 e F_3 em $\mathbb{Z}[x]$ com coeficientes liderantes positivos que satisfaçam*

$$\frac{n}{ux + v} = \frac{1}{F_1(x)} + \frac{1}{F_2(x)} + \frac{1}{F_3(x)},$$

com $n = 0 \bmod 4$.

Demonstração: Devido à sua complexidade a prova não será apresentada, podendo ser consultada pelo leitor no artigo de Schinzel, [7]. □

3.3 Propriedades das Soluções da Equação Diofantina $\frac{4}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}$

No teorema 2.2.5 pudemos ver propriedades das soluções da equação

$$\frac{n}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}$$

para $n \geq 4$. Nesta secção serão agora apresentadas mais propriedades das soluções da referida equação, mas apenas no caso em que $n = 4$. Também estas propriedades foram apresentadadas por Monks e Velingker em [4].

Vejamos então o teorema que enuncia essas propriedades:

Teorema 3.3.1 *Sejam $p > 4$ um primo e (a, b, c) uma solução de inteiros positivos para*

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \tag{3.9}$$

com $a \leq b \leq c$.

Então as seguintes propriedades verificam-se:

1. $p^2 \nmid b$ *e* $p^2 \nmid c$.
2. *Seja* $z = 4 \times mdc(a, b)$, *se* $c = p \times mmc(a, b)$, *então* $p^2 + z$ *tem um divisor congruente com* $-p \bmod z$.
3. $a = b$ *se e só se*
$$(a, b, c) = \left(\frac{p+1}{2}, \frac{p+1}{2}, \frac{p(p+1)}{4}\right)$$
e a é par. Temos ainda, que tal solução apenas existe se $p = 3 \bmod 4$.
4. $mdc(b, c) \neq 1$.
5. *Seja* $k = \frac{c}{p}$. *Então* $p \nmid b$ *se e só se* $4k = 1 \bmod p$.
6. $\left\lceil \frac{p}{4} \right\rceil \leq a \leq \frac{p+1}{2} \leq b$.
7. *Se* $p \mid b$, *então* $a \leq \left\lfloor \frac{pz}{3z-1} \right\rfloor$, *onde* $z = \left\lceil \sqrt{\left\lceil \frac{p}{4} \right\rceil} \right\rceil$.
8. $p \left\lfloor \frac{5 + \sqrt{4p-3}}{4} \right\rfloor \leq c \leq \frac{p^2(p+1)\left\lceil \frac{p}{4} \right\rceil}{4\left\lceil \frac{p}{4} \right\rceil - p}$.

Demonstração:

1. Sejam $s = \upsilon_p(b)$ e $t = \upsilon_p(c)$. Vamos começar por provar que

$$(t > 1 \text{ ou } s > 1) \Rightarrow s = t. \tag{3.10}$$

Suponhamos que $t > 1$. Por definição de υ, $b = p^s k$ e $c = p^t w$, para k, $w \in \mathbb{Z}^+$ e ainda, $p \nmid k$ e $p \nmid w$. Substituindo b e c na equação (3.9) temos:

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{p^s k} + \frac{1}{p^t w},$$

ou seja,

$$4 = \frac{p^{s+t}kw + ap^t w + ap^s k}{ap^{s+t-1}kw},$$

portanto,

$$4ap^{s+t-1}kw = p^{s+t}kw + ap^t w + ap^s k,$$

assim,

$$4ap^{s+t-1}kw - ap^t w - p^{s+t}kw = ap^s k,$$

logo,

$$(4ap^s k - ap - p^{s+1}k)p^{t-1}w = ap^s k. \tag{3.11}$$

Como, por hipótese, $t - 1 > 0$, $p \mid (4ap^s k - pa - p^{s+1}k)p^{t-1}w$ e portanto, $p \mid ap^s k$. Da parte (3.) do teorema 2.2.5, temos que $p \nmid a$ e já vimos que $p \nmid k$, então, como p é primo, pelo teorema 1.2.11, $p \mid p^s$, logo $s \geq 1$.

Da equação (3.11), temos

$$(4ap^{s-1}k - a - p^s k)p^t w = ap^s k \tag{3.12}$$

e como $s \geq 1$, $(4ap^{s-1}k - a - p^s k)w$ é inteiro, logo $p^t \mid ap^s k$. Como já vimos que $mdc(k, p) = mdc(a, p) = 1$, então $p^t \mid p^s$, logo $s \geq t$. Por transitividade, $s > 1$, logo $p \mid p^{s-1}$. Temos então

$$\begin{aligned}(4ap^{s-1}k - a - p^s k)w &= (0 - a - 0)w \bmod p \\ &= -aw \bmod p \\ &\neq 0 \bmod p.\end{aligned}$$

Ou seja, $p \nmid (4ap^{s-1}k - a - p^s k)w$ e portanto, $p^{t+1} \nmid (4ap^{s-1}k - a - p^s k)p^t w$, logo $t = \upsilon_p((4ap^{s-1}k - a - p^s k)p^t w)$. Também já vimos que $mdc(k, p) = mdc(a, p) = 1$, logo $p \nmid ak$ e portanto, $s = \upsilon_p(ap^s k)$. Pela equação (3.12), temos então que

$$t = \upsilon_p((4ap^{s-1}k - a - p^s k)p^t w) = \upsilon_p(ap^s k) = s.$$

Provou-se então que $t > 1 \Rightarrow s = t$. Como não foi feita qualquer distinção entre b e c, também se prova que $s > 1 \Rightarrow s = t$. Está então provada a implicação (3.10).

Como p é um primo maior que 4, p é ímpar e portanto, $p = 1$ ou $3 \bmod 4$. Vamos tratar os dois casos separadamente:

i) $p = 1 \bmod 4$.

Então $p = 4m - 3$, para algum $m \in \mathbb{Z}^+$. Logo

$$\frac{p}{4} = m - \frac{3}{4}$$

e portanto,

$$\left\lceil \frac{p}{4} \right\rceil = \left\lceil m - \frac{3}{4} \right\rceil = m.$$

Na observação 2.2.1 vimos que $\frac{p}{4} < a$. Mas como a é inteiro então

$$\left\lceil \frac{p}{4} \right\rceil \leq a. \tag{3.13}$$

Portanto, $m \leq a$, logo,

$$\frac{1}{a} \leq \frac{1}{m},$$

e assim,

$$\frac{1}{b} + \frac{1}{c} = \frac{4}{p} - \frac{1}{a} \geq \frac{4}{p} - \frac{1}{m} = \frac{4}{4m-3} - \frac{1}{m} = \frac{3}{m(4m-3)}. \tag{3.14}$$

Partindo agora para prova por contradição, vamos supor que $p^2 \mid b$ ou $p^2 \mid c$. Sejam s e t definidos como anteriormente. Por hipótese, temos que $s \geq 2$ ou $t \geq 2$, e em qualquer dos casos a afirmação (3.10) implica que $s = t$. Portanto, p^2 divide tanto b como c e assim $b = p^2k$ e $c = p^2w$, para $k, w \in \mathbb{Z}^+$.
Substituindo em (3.14), temos

$$\frac{1}{p^2k} + \frac{1}{p^2w} \geq \frac{3}{m(4m-3)},$$

logo,

$$\frac{1}{k} + \frac{1}{w} \geq \frac{3p^2}{m(4m-3)} = \frac{3(4m-3)^2}{m(4m-3)} = 12 - \frac{9}{m}$$

e como $m > 1$,

$$\frac{1}{k} + \frac{1}{w} \geq 12 - 9 = 3.$$

Mas sabemos também que $\frac{1}{k} \leq 1$ e $\frac{1}{w} \leq 1$ e portanto,

$$\frac{1}{k} + \frac{1}{w} \leq 2.$$

Temos portanto uma contradição. Logo $p^2 \nmid b$ e $p^2 \nmid c$.

ii) $p = 3 \bmod 4$.

Então $p = 4m - 1$, para algum $m \in \mathbb{Z}^+$. Seguindo o mesmo raciocínio do caso anterior prova-se que

$$\frac{1}{b} + \frac{1}{c} \geq \frac{1}{m(4m-1)}.$$

Supondo que $p^2 \mid b$ ou $p^2 \mid c$ e procedendo de forma análoga ao caso anterior, iríamos ver que

$$\frac{1}{p^2 k} + \frac{1}{p^2 w} \geq \frac{1}{m(4m-1)},$$

logo,

$$\frac{1}{k} + \frac{1}{w} \geq 4 - \frac{1}{m} \geq 3,$$

chegando também ao absurdo de $2 \geq 3$. Logo $p^2 \nmid b$ e $p^2 \nmid c$.

Portanto em qualquer dos casos $p^2 \nmid b$ e $p^2 \nmid c$.

2. Vamos supor que existem a, b e c que satisfazem $c = p \times mmc(a, b)$. Seja $d = mdc(a, b)$ tal que $a = nd$ e $b = md$, onde m e n são inteiros positivos. Então, pelo teorema 1.2.14, $c = nmdp$. Substituindo na equação (3.9), temos

$$\frac{4}{p} = \frac{1}{nd} + \frac{1}{md} + \frac{1}{nmdp},$$

ou seja,

$$4d = \frac{p}{n} + \frac{p}{m} + \frac{1}{nm},$$

portanto,

$$4d = \frac{pm + pn + 1}{nm},$$

logo,

$$4nmd = pm + pn + 1. \tag{3.15}$$

Portanto, n e m dividem $pm + pn + 1$ e como claramente $n \mid pn$ e $m \mid pm$, então $n \mid pm + 1$ e $m \mid pn + 1$. Sejam então

$$\begin{cases} pm + 1 &= kn \\ pn + 1 &= wm, \end{cases} \tag{3.16}$$

para k e w inteiros positivos. Resolvendo este sistema ficamos com

$$\begin{cases} n &= \dfrac{p + w}{kw - p^2} \\ m &= \dfrac{p + k}{kw - p^2}. \end{cases} \tag{3.17}$$

Substituindo $pn+1$ na equação (3.15) obtemos

$$4nmd = (p+w)m,$$

ou seja,

$$4d = \frac{p+w}{n}$$

e substituindo n, temos

$$4d = kw - p^2, \tag{3.18}$$

o que implica que $4 \mid kw - p^2$. Por (3.16), temos $p \nmid k$ e $p \nmid w$. Como n e m são inteiros, por (3.17), $p+w$ e $p+k$ são divisíveis por $z = kw - p^2$. Logo k, $w = -p \bmod z$. Da equação (3.18), verificamos que $4 \times mdc(a,b) = 4d = kw - p^2 = z$. Está então satisfeita a condição de que $p^2 + z = kw$ tem divisores congruentes com $-p \bmod z$.

3. Suponhamos que $a = b$. Então, substituindo na equação (3.9), ficamos com

$$\frac{4}{p} = \frac{2}{a} + \frac{1}{c},$$

ou seja,

$$\frac{4}{p} = \frac{2c+a}{ac},$$

portanto,

$$4ac = 2pc + pa,$$

logo,

$$2(2a-p)c = pa. \tag{3.19}$$

Uma vez que c é inteiro, $2(2a-p) \mid pa$. Logo $2 \mid pa$ e $2a-p \mid pa$ e como p é um primo maior que 4, p é ímpar, logo $mdc(2,p) = 1$ e pelo teorema 1.2.10, $2 \mid a$, ou seja, a é par.

Como pela parte (3.) do teorema 2.2.5, $mdc(a,p) = 1$, então $mdc(a,-p) = 1$. É fácil observar que

$$\forall x, y, z \in \mathbb{Z},\ mdc(x,y) = 1 \Rightarrow mdc(x, y+xz) = 1. \tag{3.20}$$

Portanto $mdc(a, 2a-p) = 1$, logo $2a-p \mid p$. Mas p é primo, e por isso existem apenas duas possibiliadades: $2a-p = p$ ou $2a-p = 1$. Mas a primeira opção implicaria $a = p$ contradizendo a parte (3.) do teorema 2.2.5. Logo $2a-p = 1$, ou seja, $a = (p+1)/2$ e por hipótese, $b = (p+1)/2$. Substituindo em (3.19) temos $c = p(p+1)/4$. Ficamos também a saber que $(p+1)/2$ é par e portanto, $4 \mid p+1$, ou seja, $p = 3 \bmod 4$.

Suponhamos agora que $p = 3 \bmod 4$. Então $p+1$ é divisível por 4 e portanto, $(p+1)/2$ e $p(p+1)/4$ são inteiros. Como

$$\frac{2}{p+1} + \frac{2}{p+1} + \frac{4}{p(p+1)} = \frac{4}{p},$$

então $\left(\frac{p+1}{2}, \frac{p+1}{2}, \frac{p(p+1)}{4}\right)$ é uma solução de inteiros positivos para a equação (3.9).

Uma vez que $p > 4$, então $\frac{p}{4} > 1$ e portanto, $\frac{p(p+1)}{4} > \frac{p+1}{2}$. Logo, temos uma solução (a, b, c) com $a = b \leq c$.

4. Suponhamos que $mdc(b, c) = 1$. A parte (3.) do teorema 2.2.5 diz que $p \mid c$, então $p \nmid b$, pois caso contrário b e c não seriam coprimos. Como p é primo, $mdc(b, p) = 1$. Então pela parte (2.) do teorema 2.2.5, $b \mid ac$. Por hipótese e pelo teorema 1.2.10, $b \mid a$, logo $b \leq a$ e como $a \leq b$, então $a = b$. Por (3.),

$$a = b = \frac{p+1}{2} \text{ e } c = \frac{p(p+1)}{4}.$$

Uma vez que c é inteiro, $4 \mid p(p+1)$ e como p é primo, $mdc(4, p) = 1$, logo $4 \mid p+1$. Portanto existe um inteiro m tal que $p + 1 = 4m$. Assim $c = pm$ e $a = b = 2m$, logo $mdc(b, c) = m$. Mas como $p + 1 > 5$, $m > 1$, e portanto, $mdc(b, c) > 1$, contrariando a hipótese. Logo $mdc(b, c) \neq 1$.

5. Na parte (3.) do teorema 2.2.5 temos que $p \mid c$, então k é inteiro. É fácil ver que $c = pk$ e efetuando esta substituição na equação (3.9) temos

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{pk},$$

ou seja,

$$\frac{4}{p} = \frac{apk + bpk + ab}{abpk},$$

portanto,

$$4abk - ab = apk + bpk$$

logo,

$$(4k - 1)ab = (a + b)pk. \tag{3.21}$$

Suponhamos que $p \nmid b$. Pela equação (3.21), $p \mid (4k-1)ab$. Pela parte (3.) do teorema 2.2.5, $p \nmid a$, logo, por hipótese e dado que p é primo, o teorema 1.2.11 garante que $p \mid 4k - 1$. Portanto, $4k - 1 = 0 \mod p$, ou seja, $4k = 1 \mod p$.

Suponhamos agora que $p \mid b$. Então existe um inteiro positivo m tal que $b = pm$. Substituindo na equação (3.21) e simplificando, obtemos:

$$(4k - 1)am = (a + b)k.$$

Por hipótese, $b = 0 \mod p$ e pela parte (3.) do teorema 2.2.5, $a \neq 0 \mod p$, logo $a+b \neq 0 \mod p$. Por (1.), $p^2 \nmid c$, logo $p \nmid k$. Portanto $p \nmid (a+b)k$, logo $p \nmid (4k-1)am$. Assim $4k - 1 \neq 0 \mod p$, ou seja, $4k \neq 1 \mod p$. Daqui sai que se $4k = 1 \mod p$, então $p \nmid b$.

6. $\left\lceil \frac{p}{4} \right\rceil \leq a$ é provado por (3.13) e $a \leq \frac{p+1}{2}$ é provado pelo teorema 2.2.4.

   Para provar que $\frac{p+1}{2} \leq b$, vejamos que como $\frac{1}{b} \leq \frac{1}{a}$, então

   $$\frac{2}{b} \leq \frac{1}{a} + \frac{1}{b} < \frac{4}{p},$$

   logo,

   $$\frac{p}{2} < b.$$

   Daqui temos que $\left\lceil \frac{p}{2} \right\rceil \leq b$. Mas como p é ímpar, $\left\lceil \frac{p}{2} \right\rceil = \frac{p+1}{2}$. Logo,

   $$\frac{p+1}{2} \leq b.$$

7. Suponhamos que $p \mid b$, então

   $$b = pk \tag{3.22}$$

   para algum $k \in \mathbb{Z}^+$.

   Pela parte (3.) do teorema 2.2.5, $p \mid c$, então

   $$c = pw \tag{3.23}$$

   para algum $w \in \mathbb{Z}^+$.

   A parte (3.) do teorema 2.2.5 diz-nos ainda que $p \nmid a$, logo $mdc(a, p) = 1$. Então, pela parte (2.) do teorema 2.2.5, $a \mid bc$. Portanto, $a \mid p^2kw$ e como a e p são coprimos, $a \mid kw$, logo $a \leq kw$. Sabemos também que $b \leq c$, ou seja, $pk \leq pw$, logo $k \leq w$ e portanto, $a \leq w^2$. Na parte (6.), vimos que $\left\lceil \frac{p}{4} \right\rceil \leq a$ e portanto, $\left\lceil \frac{p}{4} \right\rceil < w^2$, logo $\sqrt{\left\lceil \frac{p}{4} \right\rceil} \leq w$ e como $w \in \mathbb{Z}^+$, então $\left\lceil \sqrt{\left\lceil \frac{p}{4} \right\rceil} \right\rceil \leq w$. Seja $z = \left\lceil \sqrt{\left\lceil \frac{p}{4} \right\rceil} \right\rceil$, então $z \leq w$ e assim,

   $$\frac{1}{pw} \leq \frac{1}{pz}. \tag{3.24}$$

   Como $k \geq 1$, então

   $$\frac{1}{pk} \leq \frac{1}{p}. \tag{3.25}$$

   Usando as igualdades (3.22) e (3.23) na equação (3.9) temos

   $$\frac{4}{p} = \frac{1}{a} + \frac{1}{pk} + \frac{1}{pw}$$

   e pelas desigualdades (3.24) e (3.25),

   $$\frac{4}{p} \leq \frac{1}{a} + \frac{1}{p} + \frac{1}{pz},$$

logo,

$$\frac{3}{p} - \frac{1}{pz} \leq \frac{1}{a}$$

e portanto,

$$a \leq \frac{pz}{3z-1}.$$

Mas como a é inteiro positivo então

$$a \leq \left\lfloor \frac{pz}{3z-1} \right\rfloor.$$

8. Vamos começar por mostrar que $c \neq p$ através de prova por contradição. Suponhamos que $c = p$. Uma vez que por (4.), $mdc(b,c) \neq 1$, então $mdc(b,p) \neq 1$ e como p é primo, $p \mid b$, logo $p \leq b$. Mas $b \leq c = p$, logo $b = c = p$. Substituindo na equação (3.9) e resolvendo em ordem a a ficamos com $a = \frac{p}{2}$. Mas a é inteiro e p é um primo maior que 4, logo é ímpar e obviamente não é divisível por 2. Portanto temos uma contradição e $c \neq p$.

   Como, pela parte (3.) do teorema 2.2.5, c é múltiplo de p, então $c \geq 2p$.

   Vamos provar a seguir que

$$\text{Se } \exists n \in \mathbb{Z}^+ : p \geq 4n^2 - 10n + 7, \text{ então } c \geq np. \tag{3.26}$$

   A prova será feita por indução em n. A afirmação é claramente verdadeira para $n = 1$ e $n = 2$, pois $c \geq 2p$. Suponhamos agora que também é verdadeira para $n = k$, com $k \geq 2$. Vamos demonstrar que a afirmação ainda é verdadeira para $n = k + 1$. Seja $p \geq 4(k+1)^2 - 10(k+1) + 7 = 4k^2 - 2k + 1$. Por hipótese de indução, $c \geq kp$, e pela parte (3.) do teorema 2.2.5, c é múltiplo de p. Portanto, para mostrar que $c \geq (k+1)p$, basta provar que $c \neq kp$. Suponhamos então que $c = kp$, então a equação (3.9) ficaria da seguinte forma:

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{kp}.$$

   e portanto,

$$\frac{1}{a} + \frac{1}{b} = \frac{4k-1}{kp}.$$

   Pelo teorema 2.1.1, existem dois divisores u e v de kp para os quais $4k - 1 \mid u + v$. Vamos considerar três casos:

   i) Tanto u com v divisores k.

   Então $u + v \leq 2k < 4k - 1$, o que contradiz o facto de $4k - 1 \mid u + v$

ii) Tanto u com v são divisíveis por p.

Então, seja $u = pd_1$ e $v = pd_2$, com d_1 e d_2 divisores de k. Portanto, temos que $4k-1 \mid p(d_1+d_2)$. Podemos verificar que para $k \geq 2$, $4k-1 < 4k^2-2k+1 \leq p$. Assim, como p é primo, p e $4k-1$ são coprimos e então $4k-1 \mid d_1+d_2$. Mas $d_1+d_2 \leq 2k < 4k-1$, e mais uma vez temos uma contradição.

iii) Apenas um de u ou v é divisível por p.

Sem perda de generalidade suponhamos que $p \mid u$. Seja $u = pd_1$ e $v = d_2$, com d_1 e d_2 divisores de k. Para calcular os valores para a e b correspondentes à nossa escolha de u e v, vejamos que

$$\frac{4k-1}{kp} = \frac{pd_1+d_2}{\frac{kp(pd_1+d_2)}{4k-1}} = \frac{pd_1}{\frac{kp(pd_1+d_2)}{4k-1}} + \frac{d_2}{\frac{kp(pd_1+d_2)}{4k-1}} = \frac{1}{\frac{k(pd_1+d_2)}{d_1(4k-1)}} + \frac{1}{\frac{kp(pd_1+d_2)}{d_2(4k-1)}}.$$

Pela parte (3.) do teorema 2.2.5, $p \nmid a$, e portanto

$$a = \frac{k(pd_1+d_2)}{d_1(4k-1)}$$

e

$$b = \frac{kp(pd_1+d_2)}{d_2(4k-1)}.$$

Temos

$$\frac{(4k-2)d_2}{d_1} \leq k(4k-2) < 4k^2-2k+1 \leq p$$

e então,

$$b = \frac{kp(pd_1+d_2)}{d_2(4k-1)} > \frac{kp\left(\left(\frac{(4k-2)d_2}{d_1}\right)d_1+d_2\right)}{d_2(4k-1)} = kp = c,$$

o que contradiz o facto de $b \leq c$.

Como vimos, os três casos levam a uma contradição, logo $c \neq kp$ e a afirmação (3.26) é verdadeira.

Vamos agora definir $f(x) = 4x^2 - 10x + 7$. Seja r o maior número real positivo tal que $f(r) = p$, então

$$4r^2 - 10r + 7 - p = 0.$$

Aplicando a fórmula resolvente, temos

$$r = \frac{10 \pm \sqrt{10^2 - 4 \times 4(7-p)}}{8}.$$

ou seja,

$$r = \frac{10 \pm \sqrt{16p-12}}{8},$$

portanto,

$$r = \frac{10 \pm 2\sqrt{4p-3}}{8},$$

e como queremos o maior r,

$$r = \frac{5 + \sqrt{4p-3}}{4}.$$

Aplicando a afirmação (3.26), sabemos que $c \geq rp$ se r é inteiro. Se r não é inteiro, vamos ver que $p \geq f(\lfloor r \rfloor)$. Para tal $f(x)$ tem de ser crescente de $r-1$ a r. Note que a derivada de $f(x)$ é $f'(x) = 8x + 10$, o que implica que $f(x)$ é crescente para qualquer $x \geq \frac{5}{4}$. Como $p > 4$, temos

$$r \geq \frac{5 + \sqrt{17}}{4} > \frac{9}{4},$$

logo $r - 1 > \frac{5}{4}$ e portanto, $f(x)$ é crescente de $r-1$ a r, ou seja, $p \geq f(\lfloor r \rfloor)$. Portanto, $c \geq \lfloor r \rfloor p$. Em ambos os casos

$$c \geq \left\lfloor \frac{5 + \sqrt{4p-3}}{4} \right\rfloor p.$$

Para o limite superior, vejamos que como pela parte (1.) deste teorema, $p^2 \nmid c$ e pela parte (3.) do teorema 2.2.5, $p \mid c$, logo $p \nmid \frac{c}{p}$ e como p é primo, $mdc\left(\frac{c}{p}, p\right) = 1$. Então pela parte (2.) do teorema 2.2.5, $\frac{c}{p} \mid ab$. Assim $c \mid pab$ e portanto, $c \leq pab$. Sabemos que $\frac{1}{b} \geq \frac{1}{c}$, logo

$$\frac{2}{b} \geq \frac{1}{b} + \frac{1}{c} = \frac{4}{p} - \frac{1}{a}$$

e como por (6.), $\left\lceil \frac{p}{4} \right\rceil \leq a$, então

$$\frac{2}{b} \geq \frac{4}{p} - \frac{1}{\left\lceil \frac{p}{4} \right\rceil} = \frac{4\left\lceil \frac{p}{4} \right\rceil - p}{p\left\lceil \frac{p}{4} \right\rceil}$$

e portanto,

$$b \leq \frac{2p\left\lceil \frac{p}{4} \right\rceil}{4\left\lceil \frac{p}{4} \right\rceil - p}.$$

Mas por (6.), $a \leq \frac{p+1}{2}$, logo,

$$c \leq pab \leq p\left(\frac{p+1}{2}\right)\left(\frac{2p\left\lceil \frac{p}{4} \right\rceil}{4\left\lceil \frac{p}{4} \right\rceil - p}\right),$$

ou seja,

$$c \leq \frac{p^2(p+1)\left\lceil \frac{p}{4} \right\rceil}{4\left\lceil \frac{p}{4} \right\rceil - p}.$$

□

3.4 Condições para que a Conjetura seja Válida

Serão agora apresentados outros resultados de Monks e Velingker em [4], que provam a existência de condições necessárias e/ou suficientes para que a conjetura de Erdős-Straus possa ser considerada válida.

Vejamos os primeiros dois resultados:

Teorema 3.4.1 *A conjetura de Erdős-Straus é verdadeira se e só se para todo o primo p, existe a inteiro positivo tal que pa tem dois divisores cuja soma é um múltiplo de $4a - p$.*

Demonstração: Podemos verificar que a equação (3.9) pode ser escrita da seguinte forma:

$$\frac{4a-p}{pa} = \frac{1}{b} + \frac{1}{c}$$

Portanto, pelo teorema 2.1.1, provar que a equação anterior tem solução em inteiros positivos a, b e c para todo o p, ou seja, que a conjetura de Erdős-Straus é verdadeira, é equivalente a provar que para todo o primo p, existe um inteiro positivo a tal que pa tem dois divisores cuja soma é um múltiplo de $4a - p$. □

Teorema 3.4.2 *A conjetura de Erdős-Straus é verdadeira se e só se para todo o primo p, existe k inteiro positivo tal que pk tem dois divisores cuja soma é um múltiplo de $4k - 1$.*

Demonstração: Pela parte (3.) do teorema 2.2.5, sabemos que $p \mid c$. Então existe k inteiro positivo tal que $c = pk$. Substituindo na equação (3.9), podemos escrever

$$\frac{4}{p} - \frac{1}{pk} = \frac{1}{a} + \frac{1}{b}$$

ou seja,

$$\frac{4k-1}{pk} = \frac{1}{a} + \frac{1}{b}$$

Então pelo teorema 2.1.1, provar que a conjetura é verdadeira é o mesmo que provar que para todo o primo p, existe um inteiro positivo k tal que pk tem dois divisores cuja soma é um múltiplo de $4k - 1$. □

Vamos agora ver a seguinte definição:

Definição 3.4.3 *Sejam u e v inteiros positivos. Definimos a função com valor positivo α por*

$$\alpha(u,v) = \frac{4uv - u - v}{d \times mdc\left(d, \frac{4uv-u-v}{d}\right)},$$

onde $d = mdc(u,v)$

Agora podemos chegar ao seguinte teorema:

Teorema 3.4.4 *Para todo $k, w \in \mathbb{Z}^+$ existe no máximo um primo p tal que*

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{pk} + \frac{1}{pw},$$

onde a é um inteiro positivo. Tal primo p existe se e só se $\alpha(k, w)$ é primo, e nesse caso $p = \alpha(k, w)$.

Demonstração: Vamos começar por provar que se k, $w \in \mathbb{Z}^+$, $d = mdc(k, w)$ e $p > 4$ é primo, então

$$\left(\exists a \in \mathbb{Z}^+ : \frac{4}{p} = \frac{1}{a} + \frac{1}{pk} + \frac{1}{pw}\right) \text{ se e só se } \frac{4kw - k - w}{d} \mid pd. \tag{3.27}$$

Por definição de máximo divisor comum, $k = k'd$ e $w = w'd$, para algum k', $w' \in \mathbb{Z}^+$. Mais, $mdc(k', w') = 1$.

Suponhamos que existe um inteiro positivo a tal que

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{pk} + \frac{1}{pw}.$$

Resolvendo em ordem a a temos

$$a = \frac{pkw}{4kw - k - w}. \tag{3.28}$$

Substituindo k e w,

$$a = \frac{pk'w'd^2}{4k'w'd^2 - k'd - w'd} = \frac{pk'w'd}{4k'w'd - k' - w'}.$$

Como a é inteiro positivo, $4k'w'd - k' - w' \mid pk'w'd$. Já vimos que $mdc(k', w') = 1$, logo, por (3.20), $mdc(k', 4k'w'd - k' - w') = 1$ e $mdc(w', 4k'w'd - k' - w') = 1$. Portanto, pelo teorema 1.2.10, $4k'w'd - k' - w' \mid pd$. Mas

$$4k'w'd - k' - w' = \frac{4kw - k - w}{d},$$

logo,

$$\frac{4kw - k - w}{d} \mid pd.$$

Vamos agora supor que $\frac{4kw-k-w}{d} \mid pd$. Então $4kw - k - w \mid pd^2$, e como $pd^2 \mid pkw$, $4kw - k - w \mid pkw$. Portanto, existe a inteiro positivo tal que $a(4kw - k - w) = pkw$, ou seja,

$$\frac{4kw - k - w}{pkw} = \frac{1}{a},$$

isto é,

$$\frac{4}{p} - \frac{1}{pw} - \frac{1}{pk} = \frac{1}{a}$$

e portanto,

$$\frac{1}{a} + \frac{1}{pk} + \frac{1}{pw} = \frac{4}{p}$$

A afirmação (3.27) está então provada.

Note-se que pela equação (3.28),

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{pk} + \frac{1}{pw} \text{ se e só se } 4kw - k - w \mid pkw.$$

Queremos mostrar que se existe um primo p tal que $4kw - k - w \mid pkw$, então esse é o único primo para o qual a afirmação é verdadeira. Antes vamos provar que

$$\forall k, w \in \mathbb{Z}^+, 4kw - k - w > kw \tag{3.29}$$

Suponhamos que existem inteiros positivos k e w tais que $4kw - k - w \leq kw$. Então $3kw - k \leq w$, logo

$$k \leq \frac{w}{3w - 1}.$$

Como w é inteiro positivo, então

$$\frac{w}{3w - 1} < 1,$$

logo $k < 1$. Mas k é inteiro positivo e portanto temos uma contradição. Logo temos que $4kw - k - w > kw$ e a afirmação (3.29) está provada.

Suponhamos que existe um primo p tal que $4kw - k - w \mid pkw$, então existe um inteiro positivo t tal que $pkw = (4kw - k - w)t$, logo $p \mid 4kw - k - w$ ou $p \mid t$. Mas se $p \mid t$, então existe um inteiro positivo t' tal que $t = pt'$ e portanto, $kw(4kw - k - w)t'$, o que implicaria que $4kw - k - w \mid kw$, contradizendo a equação (3.29). Logo $p \mid 4kw - k - w$. Pela parte (1.) do teorema 3.3.1, temos que $mdc(k, p) = mdc(w, p) = 1$. Portanto, $mdc(d, p) = 1$, logo

$$p \mid \frac{4kw - k - w}{d}.$$

Finalmente, suponhamos que existe outro primo $q \neq p$ tal que

$$\frac{4}{q} = \frac{1}{a} + \frac{1}{qk} + \frac{1}{qw},$$

onde a é um inteiro positivo. Pela afirmação (3.27),

$$\frac{4kw - k - w}{d} \mid qd.$$

Então $p \mid qd$. Já vimos que $mdc(d,p) = 1$, logo $p \mid q$. Mas, por hipótese, p e q são primos diferentes, logo $p \nmid q$. Temos então uma contradição e $q = p$, ou seja, existe no máximo um primo p tal que

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{pk} + \frac{1}{pw}.$$

Falta provar que tal primo apenas existe se $p = \alpha(k,w)$. Como $p \mid \dfrac{4kw-k-w}{d}$, então

$$\frac{4kw-k-w}{d} = pm, \tag{3.30}$$

para $m \in \mathbb{Z}^+$. Dado que

$$\frac{4kw-k-w}{d} \mid pd,$$

temos que $m \mid d$. Logo m é um divisor comum de d e $\dfrac{4kw-k-w}{d}$. Portanto

$$m \mid mdc\left(d, \frac{4kw-k-w}{d}\right).$$

Vamos agora mostrar que

$$m = mdc\left(d, \frac{4kw-k-w}{d}\right)$$

utilizando a prova por contradição. Suponhamos que $m \neq mdc\left(d, \dfrac{4kw-k-w}{d}\right)$. Então

$$\frac{mdc\left(d, \frac{4kw-k-w}{d}\right)}{m}$$

é um divisor de d maior que 1. Por (3.30), sabemos que

$$p = \frac{4kw-k-w}{dm},$$

e por definição de máximo divisor comum, existe um inteiro positivo z tal que

$$\frac{4kw-k-w}{d} = z \times mdc\left(d, \frac{4kw-k-w}{d}\right).$$

Deste modo,

$$p = z\frac{mdc\left(d, \frac{4kw-k-w}{d}\right)}{m},$$

que é um múltiplo de um divisor de d maior que 1. Mas então $mdc(d,p) \neq 1$, contradizendo a parte (1.) do teorema 3.3.1.

Portanto, $m = mdc\left(d, \dfrac{4kw-k-w}{d}\right)$ e substituindo em (3.30) temos $p = \alpha(k,w)$. □

Este teorema leva-nos ao seguinte corolário:

Corolário 3.4.5 *Se para todo o primo p existem inteiros k e w tal que $\alpha(k, w) = p$ então a conjetura de Erdős-Straus é verdadeira.*

Demonstração: Seja $b = pk$ e $c = pw$, então, pelo teorema 3.4.4, a equação (3.9) tem solução para $p = \alpha(k, w)$, se $\alpha(k, w)$ for primo. □

Capítulo 4

Estudo Computacional

Na tentativa de provar que a conjetura de Erdős-Straus se verifica até um determinado número, foi utilizado o software *Maple 14* para programar algumas rotinas que nos permitam chegar a esse objetivo. Estas rotinas podem ser encontradas no apêndice A. Os fundamentos usados são idênticos aos da pesquisa efetuada por Swett (ver [11]), que conseguiu provar que a conjetura se verifica para qualquer $m \leq 10^{14}$.

Numa primeira fase, atendendo a resultados anteriormente apresentados como o teorema de Mordell e o corolário 3.2.2, foi programado um algoritmo que funciona como uma espécie de filtro que nos permite ter um número mais reduzido de primos que possivelmente não verifiquem a conjetura. Depois, tendo em conta o corolário 2.2.2, foi programado um algoritmo, que pretende verificar se a equação

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}, \tag{4.1}$$

com $a \leq b \leq c$ inteiros positivos, tem solução quando o p é um dos primos que sobram. O estudo foi feito até 10^9.

4.1 Filtro de Primos

Para esta fase foi programada a rotina mor(p), que verifica se um determinado número está dentro das exceções presentes no teorema de Mordell e a rotina cong(), que para cada n da forma $4k-1$ cria as listas C(n). As listas C(n) são compostas de inteiros $0 \leq m \leq 4k-2$ que verifiquem a equação

$$um + v = 0 \bmod (4k-1)$$

onde u e v são dois inteiros coprimos divisores de k. Portanto de acordo com o corolário 3.2.2, a equação (3.1) tem solução para m. Logo para qualquer primo congruente com m mod n a equação (4.1) também vai ter solução. Na tabela 4.1 podemos ver essas listas até $k = 20$, sendo que foram produzidas listas até $k = 100$.

Optou-se por começar em k=3, pois as congruências mod 3 e mod 7 já estão incluídas no teorema de Mordell. De referir que a lista pode não conter todos os números que

k	**n = 4k − 1**	**C(n)**
3	11	7,8,10
4	15	7,11,13,14
5	19	14,15,18
6	23	7,10,11,15,17,19,20,21,22
7	27	20,23,26
8	31	15,23,27,29,30
9	35	23,26,31,32,34
10	39	17,19,23,29,31,34,35,37,38
11	43	32,39,142
12	47	11,15,22,23,30,31,35,39,41,43,44,45,46
13	51	38,47,50
14	55	24,27,39,47,48,53
15	59	18,23,39,44,47,54,55,56,58
16	63	31,47,55,59,61,62
17	67	50,63,66
18	71	23,31,34,35,47,53,55,59,62,63,65,67,68,69,70
19	75	
20	79	15,37,39,47,58,59,63,69,71,74,75,77,78

Tabela 4.1: Listas C(n) para $n \leq 79$.

o corolário 3.2.2 verifica. Alguns foram excluídos de forma a aumentar a velocidade de execução do algoritmo. Isto foi feito de acordo com o seguinte:

Observação 4.1.1 *Sejam m e n da forma $4k-1$ com $m \mid n$. Se $x \in C(m)$, então se existe $y \in C(n)$ tal que $y = x \bmod n$, y pode ser excluído de $C(n)$, pois já foi verificado em $C(m)$.*

Para melhor se perceber a observação vejamos o caso $k = 19$. Neste caso $C(75)$ está vazio (ver tabela 4.1), mas 56, por exemplo, podia estar na lista pois $1(56)+19 = 0 \bmod 75$ e 1 e 19 são coprimos e divisores de k. Mas se repararmos, 15 é divisor de 75 e $56 \bmod 15 = 11$, sendo que 11 está em $C(15)$. Portanto, seria redundante ter 56 na lista $C(75)$.

Por fim, programou-se a rotina ces(l), onde l é o limite de pesquisa, que percorre todos os primos p até l, criando uma lista com aqueles para os quais a equação (4.1) poderá não ter solução. Primeiro verifica se p está nas exceções do teorema de Mordell. Se não estiver passa ao próximo primo, mas em caso afirmativo verifica se p é congruente com $x \bmod n$, para cada $x \in C(n)$ e para cada n. Assim que for encontrado um caso em que $p = x \bmod n$ passamos para o próximo primo. Mas se nenhum caso for encontrado então p é adicionado à lista e passamos ao próximo primo.

Por exemplo, o primo 7 não está nas exceções do teorema de Mordell, pois não é congruente com $1, 11^2, 13^3, 17^2, 19^2$ ou $23^3 \bmod 840$ e por isso a rotina passava a verificar

o próximo primo, 11.

Noutro exemplo, quando se chegar ao primo 1801 vamos verificar que é uma exceção do teorema de Mordell, pois $1801 = 11^2 \bmod 840$. Então, passamos à segunda fase de análise e verificamos que $1801 = 8 \bmod 11$ e $8 \in C(11)$, logo passamos ao próximo primo sem adicionar 1801 à lista.

Num último exemplo, temos o primo 13383241, que está nas exceções do teorema de Mordell, pois $13383241 = 19^2 \bmod 840$, e não é congruente com nenhum $x \bmod n$ com $x \in C(n)$, pelo menos para $n \leq 399$. Como este primo foram encontrados outros 988 com o limite de pesquisa a ser $l = 10^9$.

4.2 Algoritmo para Excluir os Restantes Primos

Para esta fase foi utilizado o teorema 2.1.1, que garante condições necessárias e suficientes para que se possa averiguar se uma certa fração pode ser escrita como a soma de duas frações unitárias. Para tal foi programada a rotina s2u(x,y). Esta rotina funciona de acordo com o teorema 2.1.1. Para cada par de divisores de y, verifica se x divide a sua soma. Quando e se tal acontecer, a verificação acaba e é indicado que a fração x/y pode ser escrita como soma de duas frações unitárias, retornando o valor 1. Se nenhum par de divisores de y é tal que a soma é divisível por x, é retornado o valor 2. Esta rotina é também utilizada no capítulo 6.

O corolário 2.2.2 garante que testar se a fração $\frac{4}{p}$ pode ser escrita como

$$\frac{4}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \tag{4.2}$$

com $a \leq b \leq c$ inteiros positivos, pode ser feito num número finito de passos. Para tal basta recorrer à rotina s2u(x,y) para verificar se

$$\frac{4}{p} - \frac{1}{a} = \frac{4a - p}{pa}$$

pode ser escrito como

$$\frac{4a - p}{pa} = \frac{1}{b} + \frac{1}{c}.$$

Se for possível então a equação (4.2) tem solução para p.

Foi então programada a rotina ces2(P), onde P é lista de primos restantes, após a aplicação do filtro de primos com a rotina ces(l). Esta rotina verifica para cada primo p da lista P, se $\frac{4}{p}$ pode ser escrito como soma de três frações unitárias. Para cada p percorre todos os valores possíveis de a, sendo que

$$\frac{p}{4} < a \leq \frac{2p + 2}{4}$$

de acordo com o teorema 2.2.4. Para cada a calcula $\frac{4a-p}{pa}$. Depois chama a rotina s2u(x,y), onde x e y são, respetivamente, o numerador e o denominador da fração referida anteriormente. Se for devolvido o valor 1, a rotina ces2(P) adiciona p a uma lista auxiliar b e

passa ao próximo primo p da lista. Se for devolvido o valor 2, passa-se ao próximo a. Se para qualquer a for devolvido o valor 2, então a equação (4.1) não tem solução para p e portanto, p não é adicionado à lista b. No fim é verificado se a lista b coincide com a lista P e, em caso afirmativo, a rotina ces2(P) devolve a frase de sucesso "Todos_Verificados".

Foi exatamente isso que sucedeu e portanto para qualquer primo $p < 10^9$ a equação (4.2) vai ter solução. E tendo em conta o lema 2.2.3 para qualquer inteiro positivo $m \leq 10^9$ também. Deste modo conseguimos provar que a conjetura de Erdős-Straus é verdadeira para qualquer $m \leq 10^9$.

Capítulo 5

Número de Soluções

Neste capítulo, iremos apresentar resultados sobre o estudo do número de soluções da equação

$$\frac{4}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}, \tag{5.1}$$

sobre a qual a conjetura de Erdős-Straus afirma ter pelo menos uma solução em inteiros positivos a, b e c para qualquer inteiro $m > 1$. O estudo foi feito por Christian Elsholtz e Terence Tao em [1], tendo sido submetido ao arxiv em 2011 e publicado em 2013.

Vamos denotar $f(m)$ como o número de soluções (a, b, c) da equação (5.1) para m. Aqui não vai ser assumido que a. b e c têm de ser distintos nem que têm de estar em qualquer ordem. Deste modo é fácil saber alguns valores de $f(m)$:

Exemplo 5.0.1

$$\begin{aligned} f(1) &= 0, \\ f(2) &= 3 \ ((1,2,2),(2,1,2) \text{ e } (2,2,1)), \\ f(3) &= 12 \ ((1,6,6),...,(2,2,3),...,(1,4,12),...), \\ f(4) &= 10, \ ((3,3,3),(2,4,4),...,(2,3,6),...) \\ &... \end{aligned}$$

Nas figuras 5.1 e 5.2 podemos ver gráficos apresentados no trabalho de Elsholtz e Tao [1]. Neles temos o valor de $f(m)$ para qualquer $m \leq 1000$ e, restringindo para primos p, o valor de $f(p)$ para qualquer $p \leq 1000$.

Um dos principais elementos do estudo de Elsholtz e Tao foi procurar descobrir os limites assintóticos superior e inferior para o valor médio do números de soluções. Outro estudo teve que ver com os limites assintóticos do número de soluções. Neste trabalho iremos utilizar a notação asintótica $X \ll Y$ ou $X = O(Y)$ para dizer que $|X| \leq CY$ para alguma constante positiva C.

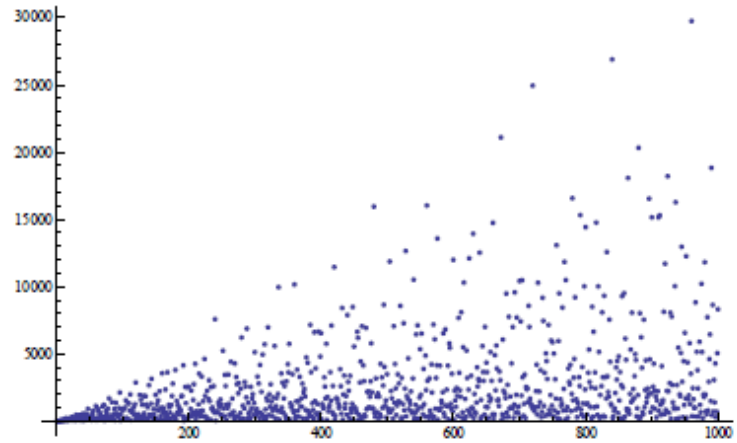

Figura 5.1: Valor de $f(m)$ para qualquer $m \leq 1000$

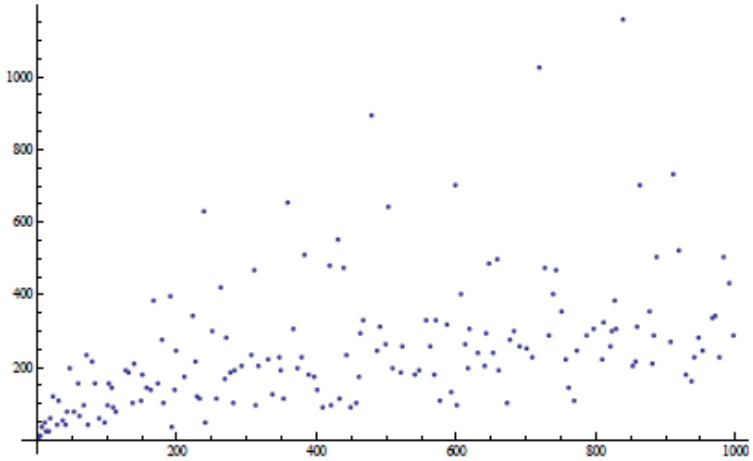

Figura 5.2: Valor de $f(p)$ para qualquer primo $p \leq 1000$

5.1 Tipos de Soluções

Podem ser definidos dois tipos de soluções em inteiros positivos (a, b, c) para a equação (5.1), de acordo com o seguinte:

Definição 5.1.1 *Dizemos que uma solução (a, b, c) para a equação (5.1) é uma* solução Tipo I *para m e denota-se $f_I(m)$, se m divide a e é coprimo com b e com c. Dizemos que é* solução Tipo II *e denota-se $f_{II}(m)$, se m divide b e c e é coprimo com a.*

Atenção, pois não é referido que as soluções ou são do tipo I ou são do tipo II. Podem existir soluções que não são de nenhum dos dois tipos. Por exemplo, para $m = 4$ existe a solução $(3, 3, 3)$, que claramente não é uma solução do tipo I nem uma solução do tipo II.

Portanto, permutando a, b e c é fácil ver que

$$f(m) \geq 3f_I(m) + 3f_{II}(m).$$

Vejamos novamente o caso $m = 4$:

Exemplo 5.1.2 *Como vimos no exemplo 5.0.1, $f(4) = 10$. Dessas 10 soluções podemos ver que nenhuma delas é do tipo I ou do tipo II, pois para $(3,3,3)$, $(2,3,6)$, $(2,6,3)$, $(3,2,6)$, $(3,6,2)$, $(6,2,3)$ e $(6,3,2)$ temos que m não divide a, b, ou c; para $(4,2,4)$ e $(4,4,2)$ temos que m divide a mas não é coprimo com b e com c e para $(2,4,4)$ temos que m divide b e c, mas m não é coprimo com a. Logo $f_I(4) = f_{II}(4) = 0$ e ficamos com $10 \geq 0$, o que está de acordo como o resultado anterior.*

Vejamos agora outro exemplo em que temos soluções de algum tipo:

Exemplo 5.1.3 *Para $m = 2$ temos uma solução do tipo II, $(1,2,2)$, sendo que as outras duas soluções, $(2,1,2)$ e $(2,2,1)$, não são de nenhum tipo. Logo $f_I(2) = 0$ e $f_{II}(2) = 1$ e ficamos com $3 \geq 3$, que está correto.*

Quando temos que $p > 4$ é um primo, sabemos que p divide pelo menos um dos inteiros a, b ou c mas não os divide todos, pois pela parte (3.) do teorema 2.2.5, sabemos p divide o maior deles e não divide o menor. Por isso podemos afirmar que

$$f(p) = 3f_I(p) + 3f_{II}(p) \tag{5.2}$$

para qualquer primo p. Os resultados do teorema 2.2.5 são para $p > 4$, mas como já vimos para $m = 2$ temos uma igualdade e como vamos ver no exemplo a seguir, para $m = 3$ também.

Exemplo 5.1.4 *No exemplo 5.0.1 vimos $f(3) = 12$. Dessas soluções 3 são do tipo I, são elas $(3,2,2)$, $(12,1,4)$ e $(12,4,1)$. Existe ainda uma solução do tipo II, $(1,6,6)$. As restantes 8 soluções não são de qualquer tipo. Temos então $f_I(3) = 3$ e $f_{II}(3) = 1$, pelo que $f(3) = 3f_I(3) + 3f_{II}(3) = 3(3) + 3(1) = 12$, confirmando o resultado.*

5.2 Valor Médio do Número de Soluções

Nesta secção iremos apresentar resultados relacionados com o valor médio do número de soluções, nomeadamente limites assintóticos para esse valor.

Vejamos então o seguinte teorema:

Teorema 5.2.1 *Quando N é suficientemente grande, podemos verificar os seguintes limites:*

$$\begin{aligned}
N\log^3 N \ll &\sum_{m<N} f_I(m) &\ll N\log^3 N\\
N\log^3 N \ll &\sum_{m<N} f_{II}(m) &\ll N\log^3 N\\
N\log^2 N \ll &\sum_{p<N} f_I(p) &\ll N\log^2 N\log\log N\\
N\log^2 N \ll &\sum_{p<N} f_{II}(p) &\ll N\log^2 N.
\end{aligned}$$

Demonstração: A prova deste teorema envolve critérios de solvabilidade das soluções do tipo I e tipo II, combinados com resultados da teoria analítica dos números, como a desigualdade de Brun-Titchmarsh e a desigualdade de Bombieri-Vinogradov. Dada a sua complexidade a prova não será apresentada, podendo ser consultada pelo leitor em [1]. □

Depois deste teorema podemos chegar a dois corolários.
Vejamos o primeiro:

Corolário 5.2.2 *O valor médio de $f(m)$ é assintoticamente maior que $\log^3 N$, ou seja,*

$$\frac{1}{N}\sum_{m<N} f(m) \gg \log^3 N.$$

Tendo em conta a equação (5.2) e dado que $\phi(N) \sim \frac{N}{\log N}$, onde $\phi(N)$ é o número de inteiros positivos menores ou iguais que N que são primos (ver [3]), podemos chegar ao segundo corolário:

Corolário 5.2.3 *Quando $N \to \infty$, o valor médio de $f(p)$ tem os seguintes limites:*

$$\log^3 N \ll \frac{\log N}{N}\sum_{p<N} f(p) \ll \log^3 N \log\log N.$$

5.3 Limites Assintóticos para o Número de Soluções

Agora serão apresentados os resultados relativos aos limites assintóticos de $f(p)$. Tal como na secção anterior, as provas estão omissas, podendo ser consultadas em [1].

Vamos começar por ver limites superiores para $f_I(m)$ e $f_{II}(m)$:

Teorema 5.3.1 *Para qualquer m inteiro positivo, temos*

$$f_I(m) \ll m^{\frac{3}{5}+O\left(\frac{1}{\log\log m}\right)}$$
$$f_{II}(m) \ll m^{\frac{3}{5}+O\left(\frac{1}{\log\log m}\right)}.$$

Recorrendo à equação (5.2), é fácil deduzir o seguinte corolário do teorema anterior:

Corolário 5.3.2 *Para qualquer primo p, temos*

$$f(p) \ll p^{\frac{3}{5}+O\left(\frac{1}{\log\log p}\right)}.$$

Vejamos agora limites inferiores de $f(m)$ para certos conjuntos de m:

Teorema 5.3.3 *Para uma quantidade infinita de m, temos*

$$f(m) \geq \exp\left((\log 3 + o(1))\frac{\log m}{\log\log m}\right),$$

onde o(1) denota uma quantidade que vai para zero quando $m \to \infty$.

Para qualquer função $\xi(m)$ que vai para $+\infty$ quando $m \to \infty$, temos

$$f(m) \geq \exp\left(\frac{\log 3}{2}\log\log m - O\left(\xi(m)\sqrt{\log\log m}\right)\right) \gg (\log m)^{0.549}$$

para m num subconjunto A de inteiros positivos de densidade 1 (isto é, $\frac{|A\cap\{...,N\}|}{N} \to 1$ quando $N \to \infty$).

No caso dos primos temos o seguinte resultado:

Teorema 5.3.4 *Para qualquer primo p num subconjunto B de primos de densidade relativa 1 (isto é, $\frac{|\{p\in B: p\leq N\}|}{|\{p: p\leq N\}|} \to 1$ quando $N \to \infty$), temos*

$$f(p) \geq \exp\left(\left(\frac{\log 3}{2} - o(1)\right)\log\log p\right) \gg (\log p)^{0.549}.$$

Capítulo 6

Generalização para Qualquer n

Neste capítulo será apresentada uma versão generalizada da conjetura de Erdős-Straus. Nesta versão é afirmado que a equação

$$\frac{n}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \tag{6.1}$$

tem solução em inteiros positivos a, b e c, com $a \leq b \leq c$, para inteiros $n > 4$ e $m > \lambda_n$, com λ_n a ser o maior m para o qual a equação (6.1) não tem solução, isto é, define-se

$$\delta_n = \left\{ m : \frac{n}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \right\}$$

e

$$\lambda_n = \sup_{m \notin \delta_n} m$$

A. Schinzel conjeturou que, para qualquer n, o número de inteiros para os quais a equação (6.1) não tem solução é finito (ver p. 178 de [8]), ou seja, $\lambda_n < \infty$.

6.1 Caso $n = 5$

Agora iremos estudar o caso $n = 5$. Para este caso, Sierpinski (ver [8]) conjeturou que

$$\frac{5}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \tag{6.2}$$

tem solução em inteiros positivos (a, b, c), com $a \leq b \leq c$, para qualquer inteiro $m > 1$.

Iremos mais à frente provar que a conjetura é verdadeira para qualquer $m \leq 10^{10}$. Vejamos o seguinte resultado, que B. M. Stewart prova em [9], através do qual se consegue restringir os inteiros para os quais a equação (6.2) poderá não ter solução:

Lema 6.1.1 *A equação (6.2) tem solução para qualquer* $m \neq 1 \bmod 278460$.

Demonstração: Se encontrarmos d_1 e d_2 nas condições do teorema 2.1.1, podemos provar que $\frac{5}{m} - \frac{1}{a} = \frac{5a-m}{ma}$ pode ser escrito como soma de duas frações unitárias, ou seja, $\frac{5}{m}$ pode ser escrito como soma de três. Vamos tomar $A = 5a - m$. Se A for 0 ou 1, basta ver a observação 2.1.2, para garantir que a equação (6.2) tem solução para m. Senão, temos de encontrar d_1 e d_2 divisores de ma tais que $A \mid d_1 + d_2$.

Seja $m = 5U + k$, com U inteiro positivo e $k \in \{0, 1, 2, 3, 4\}$. Se $k = 0$ e $a = U$, então $A = 0$ e, pela observação 2.1.2, a equação (6.2) tem solução para qualquer $m = 0 \bmod 5$. Se $k = 2$ e $a = U + 1$, então $A = 3$ e existem dois divisores de ma tais que A divide a sua soma. São eles $d_1 = m$ e $d_2 = a$, pois claramente m e a dividem ma e $m + a = 5U + 2 + U + 1 = 6U + 3 = 3(2U + 1)$ é divisível por $3 = A$. Seguindo o mesmo raciocínio temos a seguinte tabela:

k	**a**	**A**	$\mathbf{d_1}$	$\mathbf{d_2}$
0	U	0	usar 2.1.2	
2	$U+1$	3	m	a
3	$U+1$	2	m	a
4	$U+1$	1	usar 2.1.2	

Falta o caso em que $k = 1$, ou seja, em que $m = 5U + 1$. Temos então que a equação (6.2) tem solução para qualquer $m \neq 1 \bmod 5$.

Seja $U = 4V + k$, com V inteiro positivo e $k \in \{0, 1, 2, 3\}$. Através do raciocínio aplicado anteriormente, obtemos:

k	**a**	**A**	$\mathbf{d_1}$	$\mathbf{d_2}$
1	$4V+2$	4	a	2
2	$4V+3$	4	a	1
3	$4V+4$	4	m	a

Falta o caso em que $k = 0$, ou seja, em que $m = 20V + 1$. Seja $V = 3W + k$, com W inteiro positivo e $k \in \{0, 1, 2\}$. Temos agora:

k	**a**	**A**	$\mathbf{d_1}$	$\mathbf{d_2}$
1	$12W+6$	9	6	3
2	$12W+9$	4	3	1

Falta $m = 60W + 1$. Seja $W = 3D + k$, com D inteiro positivo e $k \in \{0, 1, 2\}$. Temos agora:

k	**a**	**A**	$\mathbf{d_1}$	$\mathbf{d_2}$
1	$36D+14$	9	m	2
2	$36D+26$	9	a	1

Falta $m = 360D+1$. Seja $D = 7E+k$, com E inteiro positivo e $k \in \{0, 1, ..., 6\}$. Temos agora:

k	**a**	**A**	$\mathbf{d_1}$	$\mathbf{d_2}$
1	$252E + 39$	14	$a/3$	1
2	$252E + 75$	14	$a/3$	3
3	$252E + 111$	14	a	1
4	$252E + 147$	14	a	7
5	$252E + 183$	14	$ma/3$	3
6	$252E + 219$	14	ma	1

Falta $m = 1260E + 1$. Seja $E = 13F + k$, com F inteiro positivo e $k \in \{0, 1, ..., 12\}$. Temos agora:

k	**a**	**A**	$\mathbf{d_1}$	$\mathbf{d_2}$
1	$52(63F + 5)$	39	26	13
2	$39(84F + 13)$	14	13	1
3	$4(819F + 191)$	39	$a/4$	4
4	$78(42F + 13)$	29	26	3
5	$468(7F + 4)$	3059	$234m$	$a/468$
6	$4(819F + 380)$	39	a	1
7	$52(63F + 34)$	19	$13m$	$a/26$
8	$4(819F + 506)$	39	a	4
9	$91(36F + 25)$	34	$13m$	$a/91$
10	$26(126F + 97)$	9	26	1
11	$26(126F + 107)$	49	$26m$	$a/26$
12	$234(14F + 13)$	89	$13m$	$a/26$

Vejamos melhor o caso $k = 5$. É fácil ver que $d_1 = 234m$ divide ma. Temos também que $d_2 = a/468$ divide ma, pois $d_2 = 7F + 4$ e claramente $7F + 4$ divide $ma = m468(7F + 4)$. Como $d_1 + d_2 = 234m + a/468 = 234(1260(13F + 5) + 1) + 7F + 4 = 3832927F + 1474438 = 3059(1253F + 482)$, então $A = 3059$ divide $d_1 + d_2$.

Seja agora $E = 17G + k$, com G inteiro positivo e $k \in \{0, 1, ..., 16\}$. Temos:

k	**a**	**A**	$\mathbf{d_1}$	$\mathbf{d_2}$
1	$51(84G+5)$	14	$a/51$	51
2	$102(42G+5)$	29	$17m$	$a/102$
3	$204(21G+4)$	299	$102m$	$a/102$
4	$204(21G+5)$	59	$17m$	$a/34$
5	$12(357G+107)$	119	$a/12$	12
6	$7(612G+217)$	34	$ma/7$	1
7	$68(63G+26)$	19	17	2
8	$119(36G+17)$	34	119	17
9	$34(126G+89)$	49	$17m$	$a/34$
10	$7(612G+361)$	34	$ma/7$	1
11	$102(42G+29)$	929	$51m$	$a/51$
12	$34(126G+89)$	9	17	1
13	$7(612G+469)$	34	$a/7$	7
14	$7(612G+505)$	34	a	1
15	$12(357G+317)$	119	$a/4$	1
16	$7(612G+577)$	34	$a/7$	1

Dados os dois últimos resultados, falta $m = 1260 \times 13 \times 17X + 1 = 278460X + 1$, para X inteiro positivo. Podemos então afirmar que a equação (6.2) tem solução para qualquer $m \neq 1 \bmod 278460$ □

Tendo em conta o lema anterior foi programada uma rotina em Maple que pretende encontrar primos p para os quais a equação (6.1) não tem garantidamente solução. Esta rotina, designada gen5(), percorre inteiros maiores que 1 e congruentes com 1 mod 278460 e verifica se são primos. Em caso afirmativo, percorre todos os valores de a possíveis (ver observação 2.2.1 e teorema 2.2.4) e testa se

$$\frac{5}{p} - \frac{1}{a} = \frac{5a-p}{pa}$$

pode ser escrito como soma de duas frações unitárias, até que se obtenha uma resposta positiva ou se atinja o limite superior de a. Para isso foi utilizada a rotina s2u(x,y), já descrita no capítulo 4, onde x e y são, respetivamente, o numerador e denominador de $\frac{5a-p}{pa}$. Como vimos antes, a rotina tem em conta as condições do teorema 2.1.1. O corolário 2.2.2 garante que o teste é completo e finito.

A pesquisa foi feita até $p < 10^{10}$ e para cada primo p existia pelo menos um valor a para o qual s2u(x,y) devolvia o valor 1, indicando que a fração x/y pode ser escrita como soma de duas frações unitárias.

Portanto, para todos os primos $1 < p < 10^{10}$ podemos garantir que a equação (6.2) tem solução. Tendo em conta o lema 2.2.3, podemos garantir que a equação (6.2) tem solução para qualquer inteiro $m \leq 10^{10}$.

6.2 Caso $n = 6$

Vejamos agora o caso em que $n = 6$. Neste caso surge a hipótese de que a equação

$$\frac{6}{m} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \tag{6.3}$$

tem solução inteiros positivos (a, b, c), com $a \leq b \leq c$, para qualquer inteiro $m > 1$.

Em [12], W. A. Webb chegou ao seguinte resultado:

Lema 6.2.1 *A equação (6.3) tem solução para qualquer* $m \neq 1, 61$ *ou* $541 \bmod 660$.

Demonstração: Vamos ver que se a equação (6.3) não tem solução, então $m = 6k + 1$, com k inteiro positivo. Se m é par, então $m = 2k$, com k inteiro positivo e temos:

$$\frac{6}{m} = \frac{3}{k} = \frac{1}{k} + \frac{1}{k} + \frac{1}{k}.$$

Se m é múltiplo de 3, então $m = 3k$, com k inteiro positivo e temos:

$$\frac{6}{m} = \frac{2}{k} = \frac{1}{k} + \frac{1}{2k} + \frac{1}{2k}.$$

Falta ver o caso em que $m = 6k + 5$, com k inteiro positivo. Sabemos que $a \geq \frac{m}{6}$ e que a é inteiro, portanto $a \geq k + 1$. Vamos tomar então $a = k + 1$ e ficamos com:

$$\frac{6}{6k+5} - \frac{1}{k+1} = \frac{1}{(6k+1)(k+1)},$$

portanto,

$$\frac{6}{6k+5} = \frac{1}{k+1} + \frac{1}{2(6k+1)(k+1)} + \frac{1}{2(6k+1)(k+1)}.$$

Está então provado que se a equação (6.3) não tem solução, então $m = 6k + 1$, com k inteiro positivo.

Seja então $m = 6k + 1$, com k inteiro positivo. Podemos também ver que $a \geq k + 1$ e tomando $a = k + 1$, temos

$$\frac{6}{6k+1} - \frac{1}{k+1} = \frac{5}{(6k+1)(k+1)}$$

É fácil ver que se $k = 4 \bmod 5$, então $5 \mid k + 1$ e portanto podemos escrever $\frac{5}{(6k+1)(k+1)}$ como uma fração unitária, e pela observação 2.1.2, como soma de duas. Ou seja, $\frac{6}{6k+1}$ pode ser escrita como soma de três frações unitárias.

Vamos agora encontrar inteiros d_1 e d_2 tais que, para diferentes valores de k, satisfaçam as condições do teorema 2.1.1, isto é, têm que dividir $(6k + 1)(k + 1)$ e a sua soma tem de ser divisível por 5. Temos os seguintes casos:

- Se $k = 3 \bmod 5$, então tomamos $d_1 = k + 1$ e $d_2 = 1$

- Se $k = 2 \bmod 5$, então tomamos $d_1 = (6k+1)(k+1)$ e $d_2 = 1$
- Se $k = 1 \bmod 5$, então tomamos $d_1 = (6k+1)(k+1)$ e $d_2 = 1$
- Se $k = 5 \bmod 10$, então tomamos $d_1 = (k+1)/2$ e $d_2 = 2$

Vejamos mais detalhadamente o caso em $k = 5 \bmod 10$. Nesse caso $(6k+1)(k+1) = (60k'+6)(10k'+6)$, para k' inteiro positivo, que é par, logo é divisível por d_2. Podemos ver também que $d_1 = 5k'+3$ divide $(60k'+6)(10k'+6) = (6k+1)(k+1)$. Falta ver que 5 divide $d_1 + d_2$, o que é verdade, pois $d_1 + d_2 = 5k'+5$, que claramente é múltiplo de 5.

Portanto, se a equação (6.3) não tem solução, então $k = 0 \bmod 10$, ou seja, $m = 60w+1$, com w inteiro positivo.

Repetindo o mesmo processo temos que $a \geq 10w+1$ e tomando $a = 10w+2$ temos:

$$\frac{6}{60w+1} - \frac{1}{10w+2} = \frac{11}{2(60w+1)(5w+1)}$$

Aplicando novamente o teorema 2.1.1:

- Se $w = 10 \bmod 11$ então $d_1 = 2(60w+1)(5w+1)$ e $d_2 = 1$
- Se $w = 8 \bmod 11$ então $d_1 = (60w+1)(5w+1)$ e $d_2 = 2$
- Se $w = 7 \bmod 11$ então $d_1 = (60w+1)(5w+1)$ e $d_2 = 2$
- Se $w = 6 \bmod 11$ então $d_1 = 5w+1$ e $d_2 = 2$
- Se $w = 5 \bmod 11$ então $d_1 = 2(60w+1)(5w+1)$ e $d_2 = 1$
- Se $w = 4 \bmod 11$ então $d_1 = 5w+1$ e $d_2 = 1$
- Se $w = 3 \bmod 11$ então $d_1 = 2(5w+1)$ e $d_2 = 1$

Temos ainda que se $w = 2 \bmod 11$, então $11 \mid 5w+1$, logo $\frac{6}{60w+1} - \frac{1}{10w+2}$ pode ser escrito como soma de duas frações unitárias.

Sobram portanto os casos $w = 0$, 1, ou 9 mod 11. Logo a equação (6.3) tem solução para qualquer $m \neq 1, 61$ ou 541 mod 660. □

Tal como em $n = 5$, foi programada uma rotina no *Maple 14* que pretende encontrar primos para os quais a equação (6.3) não tem garantidamente solução. Esta rotina, designada gen6() percorre primos maiores que 1 e verifica se são congruentes com 1, 61 ou 541 mod 660. Em caso afirmativo, percorre todos os valores de a possíveis e para cada um deles testa se

$$\frac{6}{p} - \frac{1}{a} = \frac{6a-p}{pa}$$

pode ser escrito como soma de duas frações unitárias, até que haja uma resposta positiva ou se atinja o limite superior de a. Para este teste foi mais uma vez utilizada a rotina s2u(x,y), onde x e y são, respetivamente, o numerador e denominador da fração acima. Como já foi dito, esta rotina foi descrita no capítulo 4 e tem em conta as condições do teorema 2.1.1, sendo que o corolário 2.2.2 garante que o teste é completo e finito.

A pesquisa foi feita até 10^7 e em todos os casos o teste foi positivo, ou seja, para todos os primos $1 < p < 10^7$ podemos garantir que a equação (6.3) tem solução. E tendo em conta o lema 2.2.3, também podemos garantir que a equação (6.3) tem solução para qualquer inteiro $1 < m \leq 10^7$.

6.3 Caso $n \geq 7$

Para o caso $\frac{n}{m}$, realizou-se um estudo que pretende procurar, para cada $n \geq 7$, primos p para os quais a equação

$$\frac{n}{p} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \tag{6.4}$$

não tem garantidamente solução. Para tal foi tido em conta o corolário 2.2.2. Foi então programado no *Maple 14* a rotina genn(n), que dado n, para cada p, percorre todos os valores de a possíveis e através da rotina s2u(x,y), verifica se

$$\frac{n}{p} - \frac{1}{a} = \frac{na - p}{pa}$$

pode ser escrito como soma de duas frações unitárias, o que, como sabemos, significaria que a equação (6.4) teria solução para p. Quando se encontrar um a para o qual a resposta da rotina s2u(x,y) seja positiva, o teste para esse p acaba e passamos ao próximo. Se a resposta por negativa para qualquer valor possível de a, então p será adicionado a uma lista que, para o n dado, vai conter os primos para os quais a equação (6.4) não tem garantidamente solução. A rotina foi chamada para $7 \leq n \leq 23$. A procura será feita apenas para $p > \frac{n}{3}$, pois é evidente que para $p < \frac{n}{3}$ não há solução e para $p = \frac{n}{3}$ a solução é $a = b = c = 1$.

Na tabela 6.1 podemos ver, para cada $7 \leq n \leq 23$, os valores de $p > \frac{n}{3}$ para os quais a equação (6.4) não tem solução.

A procura foi feita para $p < 10^5$, por isso é provável que para $n = 15$, 16 e 18 e $n \geq 20$ a lista não esteja completa, visto que os maiores primos para os quais a equação (6.1) não tem solução estão relativamente próximos do limite de pesquisa. De notar ainda que apesar da lista apenas conter primos, é possível que hajam números compostos para os quais a equação (6.1) não tem solução. Pelo lema 2.2.3, a fatorização em primos destes compostos apenas poderia ter estes primos e primos menores que n.

De notar, que para $n = 7$ não foi encontrado qualquer primo $p > 2$ para o qual a equação (6.1) não tem solução, pelo que $\lambda_7 > 2$. Para $n > 7$ podemos verificar que $\lambda_n > n$, sendo que em alguns casos pode ser mesmo bastante maior. No caso $n = 12$ podemos verificar que o último primo da lista é 12241, um número bastante superior a 12, no entanto para

$12241 < p \leq 100000$ não foi detetado qualquer contraexemplo. Esta análise pode então dar razões a favor da conjetura generalizada de que $\lambda_n < \infty$ para qualquer n. No entanto o já referido facto de, por exemplo, $n = 20$ ter um último primo da lista próximo do limite de pesquisa, pode também dar razões contra a conjetura.

n	**p**
7	-
8	3, 11, 17, 131, 241
9	5, 11, 19
10	7, 11, 43, 61, 67, 181
11	37
12	5, 7, 13, 29, 31, 37, 73, 97, 193, 433, 577, 1129, 1657, 1873, 2521, 2593, 3433, 10369, 12049, 12241
13	5, 7, 53, 61, 67, 79, 211, 281
14	5, 17, 19, 29, 59, 257, 353
15	17, 19, 23, 31, 47, 53, 61, 79, 113, 137, 151, 197, 233, 271, 541, 1103, 1171, 1367, 4201, 6301, 12601, 16831, 20521
16	7, 11, 13, 17, 23, 37, 73, 97, 113, 131, 167, 193, 241, 257, 421, 577, 593, 641, 769, 1201, 1489, 2113, 2521, 2689, 3169, 3361, 4801, 4993, 5281, 8161, 8641, 33601, 36529, 78721, 83449
17	7, 13, 19, 23, 41, 43, 53, 71, 73, 157, 281, 421, 1123, 2081
18	7, 11, 13, 19, 23, 29, 31, 37, 41, 47, 59, 61, 73, 109, 113, 131, 137, 149, 181, 193, 223, 239, 281, 379, 389, 397, 433, 457, 541, 599, 613, 661, 761, 811, 821, 911, 1009, 1297, 1381, 2269, 2819, 9461, 16561, 17389, 28081, 35281
19	7, 11, 13, 23, 29, 41, 43, 97, 137, 181, 193, 229, 353
20	7, 11, 23, 29, 41, 43, 47, 61, 67, 83, 89, 103, 107, 127, 149, 163, 167, 181, 223, 241, 347, 383, 401, 421, 503, 601, 641, 761, 809, 887, 907, 1049, 1201, 1451, 1607, 1801, 2161, 2341, 2521, 2687, 2801, 3121, 3467, 4201, 4507, 4801, 4967, 5441, 5521, 5641, 6361, 8161, 8761, 15601, 21841, 22441, 24481, 33601, 87961, 90001
21	11, 13, 17, 23, 29, 43, 89, 97, 101, 113, 127, 211, 269, 353, 401, 463, 593, 601, 757, 761, 947, 967, 1031, 7151, 14051
22	13, 17, 19, 23, 31, 37, 47, 53, 59, 61, 67, 89, 97, 101, 103, 137, 139, 151, 179, 223, 227, 229, 269, 283, 313, 331, 353, 397, 401, 487, 617, 683, 811, 929, 1021, 1237, 1321, 1327, 1459, 1901, 2017, 2861, 3433, 4013, 4621, 4657, 5569, 8009, 8647, 14543
23	13, 29, 31, 37, 41, 47, 71, 73, 101, 127, 139, 151, 163, 167, 233, 257, 277, 347, 397, 443, 463, 509, 599, 691, 829, 859, 991, 1061, 1381, 1553, 1613, 1657, 2281, 2417, 3361, 3709, 3803, 5153, 6947, 8419, 11617, 31771

Tabela 6.1: Lista que contém, para cada $7 \leq n \leq 23$, os valores de $p > \frac{n}{3}$ para os quais a equação (6.4) não tem solução.

Capítulo 7

Generalização para Somas/Subtrações

Neste capítulo será apresentada outra generalização da conjetura de Erdős-Straus. Esta generalização é estudada por Sierpinski em [8], onde o autor estuda formas de escrever números racionais como somas e subtrações de frações unitárias. No âmbito deste trabalho, apenas nos interessa estudar aqueles que se conseguem escrever com três frações unitárias, ou seja, inteiros positivos n e m da forma

$$\frac{n}{m} = \frac{1}{a} \pm \frac{1}{b} \pm \frac{1}{c}, \tag{7.1}$$

para a, b e c inteiros positivos.

André Schinzel, aluno de Sierpinski, conjeturou que para qualquer n, existe um inteiro positivo μ_n, tal que para qualquer $m > \mu_n$, a equação (7.1) tem solução em inteiros positivos (a, b, c). Esta conjetura já foi provada para qualquer $n < 36$, por B. M. Stewart e W. A. Webb em [10]. A seguir vamos ver que para alguns inteiros positivos n, essa conjetura pode ser provada facilmente, sendo que vamos ver as provas para $1 \leq n \leq 9$. Noutros casos, a prova é mais complicada e, por isso, em particular, iremos ver o caso $n = 18$.

7.1 Provas para $1 \leq n \leq 9$

A seguir são apresentadas provas de que a conjetura é válida para os casos em que $1 \leq n \leq 9$.

Seja m um qualquer inteiro positivo, é evidente que para $n = 1$,

$$\frac{1}{m} = \frac{1}{m} + \frac{1}{m} - \frac{1}{m},$$

para $n = 2$,

$$\frac{2}{m} = \frac{1}{m} + \frac{1}{m} = \frac{1}{m} + \frac{1}{2m} + \frac{1}{2m}.$$

e para $n = 3$,

$$\frac{3}{m} = \frac{1}{m} + \frac{1}{m} + \frac{1}{m}.$$

Mais à frente, vai ser útil ver que $\frac{3}{m}$ também se escreve com somas/subtrações de apenas duas frações unitárias para qualquer $m > 1$. Basta notar que se m é múltiplo de 3, então $m = 3k$, com k inteiro positivo, e temos

$$\frac{3}{m} = \frac{1}{k} = \frac{1}{2k} + \frac{1}{2k}.$$

Se m não é múltiplo de 3, então $m = 3k \pm 1$, com k inteiro positivo, e temos

$$\frac{3}{m} = \frac{3}{3k \pm 1} = \frac{1}{k} \mp \frac{1}{k(3k \pm 1)}.$$

Para $n = 4$, se m é par, então $m = 2k$, com k inteiro positivo, e temos

$$\frac{4}{m} = \frac{4}{2k} = \frac{1}{k} + \frac{1}{k} = \frac{1}{k} + \frac{1}{2k} + \frac{1}{2k}.$$

Se $m > 1$ e m é ímpar, então $m = 4k \pm 1$, com k inteiro positivo, e temos

$$\frac{4}{m} = \frac{4}{4k \pm 1} = \frac{1}{k} \mp \frac{1}{k(4k \pm 1)} = \frac{1}{2k} + \frac{1}{2k} \mp \frac{1}{k(4k \pm 1)}.$$

Portanto, se $n = 4$, a equação (7.1) tem solução para qualquer $m > 1$.

Como vimos, se $n = 4$ conseguimos escrever $\frac{4}{m}$, não só como somas/subtrações de três frações unitárias, mas também como somas/subtrações de duas frações unitárias, para qualquer inteiro $m > 1$. Portanto é fácil ver que conseguimos escrever $\frac{5}{m}$ como somas/subtrações de três frações unitárias para qualquer $m > 1$. Basta notar que

$$\frac{5}{m} = \frac{4}{m} + \frac{1}{m}$$

e $\frac{4}{m}$ pode ser escrito com somas/subtrações de duas frações unitárias.

Vejamos agora o caso $n = 6$. Para m múltiplo de 3, ou seja, para $m = 3k$, com k inteiro positivo, temos que $\frac{6}{m} = \frac{2}{k}$ e como já vimos, $\frac{2}{k}$ pode ser escrito com duas frações unitárias, logo também com três, para qualquer inteiro positivo k. Para m par, ou seja, para $m = 2k$, com k inteiro positivo, temos que $\frac{6}{m} = \frac{3}{k}$ e já vimos que $\frac{3}{k}$ pode ser escrito com três frações unitárias para qualquer k. Falta ver o caso em que $m > 1$ e $m = 6k \pm 1$, para k inteiro positivo. Nesse caso temos

$$\frac{6}{m} = \frac{6}{6k \pm 1} = \frac{1}{k} \mp \frac{1}{k(6k \pm 1)} = \frac{1}{2k} + \frac{1}{2k} \mp \frac{1}{k(6k \pm 1)}.$$

Portanto, se $n = 6$, a equação (7.1) tem solução para qualquer $m > 1$.

Vimos que, para $m > 1$, $\frac{6}{m}$ também pode ser escrito como somas/subtrações de duas frações unitárias, quando $m = 3k$ ou $m = 6k \pm 1$, para qualquer k inteiro positivo. Mas o mesmo acontece para $m = 2k$, com $k > 1$, ou seja, $m > 2$, pois vimos que $\frac{3}{k}$ pode ser escrito como somas/subtrações de duas frações unitárias para qualquer $k > 1$. Se seguirmos o mesmo raciocínio do caso $n = 5$, temos que, se $n = 7$, a equação (7.1) tem solução para qualquer $m > 2$.

No caso $n = 8$, temos que, para $m > 2$, se m é par, então $m = 2k$, com $k > 1$ inteiro e basta olhar para o caso $n = 4$, que garante que a equação (7.1) tem solução para qualquer $k > 1$. Se $m > 3$ e m é ímpar, então ou $m = 8k \pm 1$, com k inteiro positivo, e temos

$$\frac{8}{m} = \frac{8}{8k \pm 1} = \frac{1}{2k} + \frac{1}{2k} \mp \frac{1}{k(8k \pm 1)},$$

ou $m = 8k \pm 3$, com k inteiro positivo, e nesse caso temos

$$\frac{8}{m} = \frac{8}{8k \pm 3} = \frac{1}{k} \mp \frac{1}{k(3k \pm 1)} \mp \frac{1}{(3k \pm 1)(8k \pm 3)}.$$

Podemos ver que $\frac{8}{3}$ não se pode escrever com três frações unitárias. Basta notar que para tal ser possível teríamos que ter só somas e dois dos denominadores teriam que ser 1, caso contrário a soma das três frações seria sempre inferior a $\frac{8}{3}$. Mas nesse caso teríamos que a terceira fração seria igual a $\frac{8}{3} - 2 = \frac{2}{3}$, que claramente não pode ser uma fração unitária. Portanto, se $n = 8$, a equação (7.1) tem solução para qualquer $m > 3$.

Por fim, vamos ver como se prova o caso $n = 9$. Se m é múltiplo de 3, então $m = 3k$, com k inteiro positivo e basta olhar para o caso $n = 3$, que garante que a equação (7.1) tem solução para qualquer k. Se $m > 4$ e m não é múltiplo de 3 então ou $m = 9k \pm 1$, com k inteiro positivo, e temos

$$\frac{9}{m} = \frac{8}{8k \pm 1} = \frac{1}{2k} + \frac{1}{2k} \mp \frac{1}{k(9k \pm 1)},$$

ou $m = 9k \pm 2$, com k inteiro positivo, e temos

$$\frac{9}{m} = \frac{9}{9k \pm 2} = \frac{1}{k} \mp \frac{1}{k(9k \pm 2)} \mp \frac{1}{k(9k \pm 2)},$$

ou então $m = 9k \pm 4$, com k inteiro positivo, e nesse caso temos

$$\frac{9}{m} = \frac{9}{9k \pm 4} = \frac{1}{k} \mp \frac{1}{k(2k \pm 1)} \pm \frac{1}{(2k \pm 1)(9k \pm 4)}.$$

Podemos ainda ver que

$$\frac{9}{4} = \frac{1}{1} + \frac{1}{1} + \frac{1}{4}.$$

Portanto, se $n = 9$, a equação (7.1) tem solução para qualquer $m > 2$.

7.2 Caso $n = 18$

Nesta secção vamos ver um caso mais complicado, o caso em que $n = 18$. Queremos provar que existe um inteiro positivo μ_{18} tal que a equação

$$\frac{18}{m} = \frac{1}{a} \pm \frac{1}{b} \pm \frac{1}{c} \tag{7.2}$$

tem solução em inteiros positivos (a, b, c) para qualquer $m > \mu_{18}$.

É fácil verificar que, se m é par ou um múltiplo de 3, basta ter em conta os resultados para $n = 9$ e $n = 6$, respetivamente. Se m não se enquadra em nenhum desses casos, então podemos ver que $m = 108t \pm s$, com t inteiro e $s = 1$, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49 ou 53. Temos também que, para $m > 25$, basta ver os casos em que m é da forma $18k \pm 1$, $36k \pm 5$, $36k \pm 7$, $54k \pm 5$, $54k \pm 7$, $54k \pm 11$, $54k \pm 23$, $108k \pm 13$ ou $108k \pm 25$, com k inteiro positivo. Vejamos então que

$$\begin{aligned}
\frac{18}{18k \pm 1} &= \frac{1}{2k} + \frac{1}{2k} \mp \frac{1}{k(18k \pm 1)}, \\
\frac{18}{36k \pm 5} &= \frac{1}{2k} \mp \frac{1}{2k(7k \pm 1)} \pm \frac{1}{2(7k \pm 1)(36k \pm 5)}, \\
\frac{18}{36k \pm 7} &= \frac{1}{2k} \mp \frac{1}{2k(5k \pm 1)} \pm \frac{1}{2(5k \pm 1)(36k \pm 7)}, \\
\frac{18}{54k \pm 5} &= \frac{1}{3k} \mp \frac{1}{3k(11k \pm 1)} \mp \frac{1}{3(11k \pm 1)(54k \pm 5)}, \\
\frac{18}{54k \pm 7} &= \frac{1}{3k} \mp \frac{1}{k(23k \pm 3)} \pm \frac{1}{3(23k \pm 3)(54k \pm 7)}, \\
\frac{18}{54k \pm 11} &= \frac{1}{3k} \mp \frac{1}{3k(5k \pm 1)} \mp \frac{1}{3(5k \pm 1)(54k \pm 11)}, \\
\frac{18}{54k \pm 23} &= \frac{1}{3k} \mp \frac{1}{k(7k \pm 3)} \pm \frac{1}{3(7k \pm 3)(54k \pm 23)}, \\
\frac{18}{108k \pm 13} &= \frac{1}{6k} \mp \frac{1}{2k(25k \pm 3)} \mp \frac{1}{6(25k \pm 3)(108k \pm 13)}, \\
\frac{18}{108k \pm 25} &= \frac{1}{6k} \mp \frac{1}{2k(13k \pm 3)} \mp \frac{1}{6(13k \pm 3)(108k \pm 25)}.
\end{aligned}$$

Temos também que

$$\frac{18}{25} = \frac{1}{2} + \frac{1}{5} + \frac{1}{50}.$$

Podemos então afirmar que a equação (7.2) tem solução para qualquer $m > 23$.

Falta ainda ver que de facto, $\mu_{18} = 23$. Para isso temos de provar que a equação (7.2) não tem solução para $m = 23$. Suponhamos que existia solução, então teríamos três casos:

i) $\frac{18}{23} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}$.

Suponhamos que $a \leq b \leq c$. Pela observação 2.2.1, temos que

$$1 < \frac{23}{18} < a \leq \frac{69}{18} < 4$$

e como a é inteiro, $a = 2$ ou $a = 3$.

Se $a = 2$, então

$$\frac{18}{23} - \frac{1}{2} = \frac{13}{46} = \frac{1}{b} + \frac{1}{c} \leq \frac{2}{b},$$

logo $b \leq \frac{92}{13} < 8$ e como $\frac{13}{46} > b$, então $b > \frac{46}{13} > 2$. Dado que b é inteiro, então $b = 3$, 4, 5, 6 ou 7. Mas, para qualquer destes valores de b, temos que

$$c = \frac{1}{\frac{13}{46} - \frac{1}{b}}$$

não vai ser inteiro.

Se $a = 3$ e seguindo o mesmo raciocínio, temos que $b = 3$ ou $b = 4$ e, para qualquer destes valores, temos que

$$c = \frac{1}{\frac{31}{69} - \frac{1}{b}}$$

não vai ser inteiro.

Assim se conclui a prova para o caso i).

ii) $\frac{18}{23} = \frac{1}{a} + \frac{1}{b} - \frac{1}{c}$.

Suponhamos que $a \leq b$, então $\frac{18}{23} < \frac{2}{a}$ e portanto, $a < \frac{23}{9} < 3$. Como a é inteiro positivo, $a = 1$ ou $a = 2$.

Se $a = 1$, então

$$\frac{18}{23} - 1 = -\frac{5}{23} = \frac{1}{b} - \frac{1}{c},$$

donde

$$\frac{5}{23} = \frac{1}{c} - \frac{1}{b} < \frac{1}{c},$$

logo $c < \frac{23}{5} < 5$ e como c é inteiro, $c = 1$, 2, 3 ou 4. Mas, para qualquer destes valores de c, temos que

$$b = \frac{1}{\frac{1}{c} - \frac{5}{23}}$$

não vai ser inteiro.

Se $a = 2$, então

$$\frac{18}{23} - \frac{1}{2} = \frac{13}{46} = \frac{1}{b} - \frac{1}{c} < \frac{1}{b},$$

logo $b < \frac{46}{13} < 4$. Mas como $b \geq a = 2$, então $b = 2$ ou $b = 3$ e, para qualquer destes valores, temos que

$$c = \frac{1}{\frac{1}{b} - \frac{13}{46}}$$

não vai ser inteiro.

Assim se conclui a prova para o caso ii).

iii) $\frac{18}{23} = \frac{1}{a} - \frac{1}{b} - \frac{1}{c}$.

Sabemos que, neste caso, $\frac{18}{23} < \frac{1}{a}$, logo $a < \frac{23}{18} < 2$ e como a é inteiro positivo então $a = 1$. Ficamo então com

$$\frac{18}{23} - \frac{1}{2} = -\frac{5}{23} = -\frac{1}{b} - \frac{1}{c}.$$

Se supormos que $b \leq c$, então $\frac{5}{23} \leq \frac{2}{b}$, logo $b \leq \frac{46}{5} < 10$. Ficamos também a saber que $\frac{5}{23} > \frac{1}{b}$, logo $b > \frac{23}{5} > 4$ e portanto, $b = 5$, 6, 7, 8 ou 9. Mas, para qualquer destes valores de b, temos que

$$c = \frac{1}{\frac{5}{23} - \frac{1}{b}}$$

não vai ser inteiro.

Assim se conclui a prova para o caso iii).

Em qualquer dos três casos ficou provado que a equação (7.2) não tem solução para $m = 23$, pelo que se pode garantir que $\mu_{18} = 23$. Portanto, a equação (7.2) tem solução para qualquer $m > 23$.

Bibliografia

[1] Elsholtz C., Tao T., *Counting the Number of Solutions to the Erdős-Straus Equation on Unit Fractions*, J.Aust. Math. Soc. 94, pp.50-105, 2013.

[2] Erdős P., *Az* $\frac{1}{x_1} + \frac{1}{x_2} + ... + \frac{1}{x_n} = \frac{a}{b}$ *egyenlet egész számú megoldásairól*, Matematiki Lapok 1, pp. 192-210, 1950.

[3] Hardy G. H., Wright E. M., *An Introduction to the Theory of Numbers*, Oxford University Press, 2008.

[4] Monks M., Velingker A., *On the Erdős-Straus Conjecture: Properties of Solutions to its Underlying Diophantine Equation*, Siemens Westinghouse Competition, 2004-2005.

[5] Mordell, L. J., *Diophantine Equations*, Academic Press, pp. 287-290, 1968.

[6] Obláth M. R. *Sur l'équation diophantienne* $\frac{a}{b} = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$, Mathesis 59, pp. 308-316, 1950.

[7] Schinzel A., *On Sums of Three Unit Fractions with Polynomial Denominators*, Functiones et Approximatio. Commentarii Mathematici XXVII, pp. 187-194, 2000.

[8] Sierpinski W. *Sur les décompositions de nombres rationnels en fractions primaires*, Oeuvres Choisies, pp 169-184, 1974.

[9] Stewart B. M., *Egyptian Fractions*, Theory of Numbers, pp. 198-207, 1964.

[10] Stewart B. M., Webb W. A., *Sums of fractions with bounded numerators*, Canadian J. Math. 18, pp. 999-1003, 1966.

[11] Swett A., *The Erdős-Straus Conjecture*, Rev. 10/28/99.
http://math.uindy.edu/swett/esc.htm

[12] Webb W. A., *Rationals Not Expressible As a Sum of Three Unit Fractions*, Elemente der Mathematik 29, pp. 1-6, 1974.

Apêndice A

Rotinas Maple

A.1 mor(p)

```
> mor := proc (p)
> if (p mod 840 in {1, 121, 169, 289, 361, 529}) then
> return false;
> end if;
> end proc;
```

A.2 cong()

```
> cong:=proc()
> a:=[];b:=[];
> for k  from 3 to  100 do
> n:=4*k-1;
> for x in divisors(k) do
> for y in divisors(k) do
> if(gcd(x,y)=1) then
> z:=-4*k*y/x mod n;
> if(member(z,b)=false) then
> t:=true;
> for j from 1 to nops(a) do
> if(a[j][1] in divisors(n)) then
> if(member(z mod a[j][1],a[j][2])) then
> t:=false;
> break; end if; end if; end do;
> if(t=true) then
> b:=[op(b),z];
> end if; end if; end if; end do; end do;
> if(nops(b)<>0) then
> a:=[op(a),[n,b]];
> end if;
> b:=[];
> end do;
> return a;
> end proc;
```

A.3 ces(l)

```
> ces:=proc(l)
> p:=1;
> a:={};
> c:=cong();
> while(p<l) do
> p:=nextprime(p);
> b:=false;
> if(mor(p)=false)then
> for i from 1 to nops(c) do
> if(member(p mod c[i][1],c[i][2])) then
> b:=true;
> break;
> end if;
> end do;
> if(b=false) then
> a:=a union {p};
> end if;
> end if;
> end do;
> return a;
> end proc;
```

A.4 s2u(x,y)

```
> s2u:=proc(x,y)
> t:=false;
> for a in divisors(y) do
> for b in divisors(y) do
> if (b>a)then
> break;
> end if;
> if(x in divisors(a+b))then
> t:=true;
> return 1;
> break;
> end if;
> end do;
> if(t=true)then
> break;
> end if;
> end do;
> if(t=false)then
> return 2;
> end if;
> end proc;
```

A.5 ces2(P)

```
> ces2:=proc(P)
> b:={};
> for i from 1 to nops(P)do
> x:=floor(P[i]/4)+1;
> s:=2;
> while(s=2) do
> y:=4/P[i]-1/x;
> if(gcd(numer(y),denom(y))=1)then
> s:=s2u(numer(y),denom(y));
> end if;
> if(s=1)then
> b:=b union {P[i]}
> end if;
> x:=x+1;
> if(x>floor((2*P[i]+2)/4))then
> break;
> end if;
> end do;
> end do;
> if(b=P) then
> print(Todos_Verificados);
> end if;
> end proc;
```

A.6 gen5()

```
> gen5:=proc()
> p:=1;
> a:=[];
> while(p<10^10) do
> p:=p+278460;
> if(isprime(p))then
> x:=floor(p/5)+1;
> s:=2;
> while(s=2) do
> y:=5/p-1/x;
> if(gcd(numer(y),denom(y))=1)then
> s:=s2u(numer(y),denom(y));
> end if;
> x:=x+1;
> if(x>floor((2*p+2)/5) and s=2)then
> a:=[op(a),p];
> break;
> end if; end do; end if; end do;
> if(a=[]) then
> print("Todos Verificados");
> end if;
> end proc;
```

A.7 gen6()

```
> gen6:=proc()
> p:=1;
> a:=[];
> while(p<10^7) do
> p:=nextprime(p);
> if(p mod 660 in {1,61,541})then
> x:=floor(p/6)+1;
> s:=2;
> while(s=2) do
> y:=6/p-1/x;
> if(gcd(numer(y),denom(y))=1)then
> s:=s2u(numer(y),denom(y));
> end if;
> x:=x+1;
> if(x>floor((2*p+2)/6) and s=2)then
> a:=[op(a),p];
> break;
> end if; end do; end if; end do;
> if(a=[]) then
> print("Todos Verificados");
> end if;
> end proc;
```

A.8 genn(n)

```
> genn:=proc(n)
> p:=floor(n/3);
> a:=[];
> while(p<10^5) do
> p:=nextprime(p);
> x:=floor(p/n)+1;
> s:=2;
> while(s=2) do
> y:=n/p-1/x;
> if(gcd(numer(y),denom(y))=1)then
> s:=s2u(numer(y),denom(y));
> end if;
> x:=x+1;
> if(x>floor((2*p+2)/n) and s=2)then
> a:=[op(a),p];
> break;
> end if;
> end do;
> end do;
> print(a);
> end proc;
```